Exhibit

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/430,985	11/01/1999	REUVEN ROZENTUL	081/01251	8073

7590 01/17/2003

WILLIAM H. DIPPERT
REED SMITH LLP
599 LEXINGTON AVE
29th
NEW YORK, NY 10022

Response filed
2 April 2003
to

DOCKETED

EXAMINER
GANTT, ALAN T

ART UNIT	PAPER NUMBER
2684	

DATE MAILED: 01/17/2003

L.C. to
3 month Office Action
April 17, 2003

Please find below and/or attached an Office communication concerning this application or proceeding.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In regard to the application of: Ofer SHALEM et al.

Serial No : 09/504,018 Group Art Unit: 2685

Filed : February 18, 2000 Examiner: WARD, R. J.

For : INCREASING CHANNEL CAPACITY IN FIXED CELLULAR NETWORKS

INFORMATION DISCLOSURE STATEMENT

Hon. Commissioner of Patents and Trademarks
Washington, DC 20231

Sir:

The Examiner is respectfully requested to review and consider this art, in accordance with MPEP 2001.06 and to indicate in the first office action that he has considered this art. Additionally, the Examiner is respectfully requested to cite those prior art publications mentioned in this application which the Examiner considers to be material or relevant to the present claims.

Further, in order to comply with discretionary regulations 37 CFR 1.97 and 1.98, attached is an Equivalent to Form PTO-1449 listing the cited art. Also attached are copies[1] of the art. This art contains information which the Examiner may consider to be important in deciding whether to allow the present application to issue as a patent.

Applicants wish to point that items 1-5 listed on the attached equivalent to Form PTO-1449 were cited in an Office Communication dated January 17, 2003 from the U.S. Patent Office in a related U.S. Application No. 09/430,985. Copy of these items are attached herewith.

In accordance with MPEP Section 609 it is requested that each document cited [including any mentioned in Applicant's specification which is not repeated on the attached (or prior) PTO-1449 form(s) or equivalents thereof] be given thorough consideration and be cited of record in the prosecution history of the present application by initialing on the PTO-1449

[1] To the extent that a document is listed and no copy of same is attached, then such document is not at the present time available to the undersigned or is available in the national stage file. If a listed document is not in the English language and an English translation is readily available, such translation is also attached; if translation is not attached, it is not readily available to the undersigned. If a foreign language patent document is cited, and an English language equivalent is known to the undersigned, then such an equivalent patent is also cited on the attached form along with the corresponding foreign language patent and a connecting arrow indicated therebetween; if no such English language equivalent is cited then none is known to the undersigned.

form or its equivalent, so that it will appear on the face of the patent issuing on the present application, even if the Examiner does not consider it sufficiently pertinent to use in a rejection, or otherwise does not believe that the guidelines for citation have been fully complied with.

The present Information Disclosure Statement is being submitted in compliance with 37 CFR 1.56 as an Examiner might consider any cited document important in deciding whether to allow the application to issue as a patent, but the citation of each document is not to be construed as an admission that such document is necessarily relevant or prior art. No representation is intended that the cited documents represent the results of a complete search, and it is anticipated that the Examiner in the normal course of examination, will make an independent search and will determine the best prior art consistent with 37 CFR 1.104(a), and in the course of such search will review for relevance every document cited on the attached form.

Early and favorable consideration is earnestly solicited.

Respectfully submitted,
Ofer SHALEM

Paul Fenster

Paul FENSTER
Registration No. 33,877

April 14, 2003
William H. Dippert, Esq.
Reed Smith LLP
599 Lexington Avenue, 29th Floor
New York, NY 10022-7650

Tel: (212) 521-5400

US006061346A

United States Patent [19]

Nordman

[11] Patent Number: 6,061,346

[45] Date of Patent: May 9, 2000

[54] **SECURE ACCESS METHOD, AND ASSOCIATED APPARATUS, FOR ACCESSING A PRIVATE IP NETWORK**

[75] Inventor: **Mikael Nordman**, Sollentuna, Sweden

[73] Assignee: **Telefonaktiebolaget LM Ericsson (publ)**, Stockholm, Sweden

[21] Appl. No.: **08/784,152**

[22] Filed: **Jan. 17, 1997**

[51] **Int. Cl.**[7] **H04L 12/66**

[52] **U.S. Cl.** **370/352**

[58] **Field of Search** 370/351, 310, 370/328, 338, 392, 352–356; 395/200.47, 200.48, 900.54; 455/422

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,317,568	5/1994	Bixby et al.	370/401
5,559,800	9/1996	Mousseau et al.	370/401
5,812,552	9/1998	Arora et al.	370/401
5,828,844	10/1998	Civanlar et al.	395/200.58

FOREIGN PATENT DOCUMENTS

0 483 547 A1	5/1992	European Pat. Off. .
WO 94/11849	5/1994	WIPO .
PCT/SE98/00022	4/1998	WIPO .

OTHER PUBLICATIONS

Proposed Operation of GSM Packet Radio Networks by Jari Hämäläinen and Hannu H. Kari, XP 002020137; IEEE Int'l. Symposium on Personal, Indoor & Mobile Radio Communications, vol. 1, Sep. 27, 1995; pp. 372–377.

GPRS, General Packet Radio Service by Sven Åkesson, XP 000645966; Int'l. Conf. on Universal Personal Communications, Nov. 6, 1995; pp. 640–643.

Nomadic Access to Information Services by GSM Phone by Markku Kylänpää, Olli Pihlajamaa and Martin Bergenwall, XP 002037372; Computer & Graphics, vol. 20, No. 5, Sep. 1, 1996; pp. 651–658.

IP Addressing and Routing in a Local Wireless Network by Danny Cohen, Jonathan B. Postel and Raphael Rom; IEEE; XP002020138; One World Through Communications, Florence, May 4–8, 1992, vol. 2; pp. 626–632.

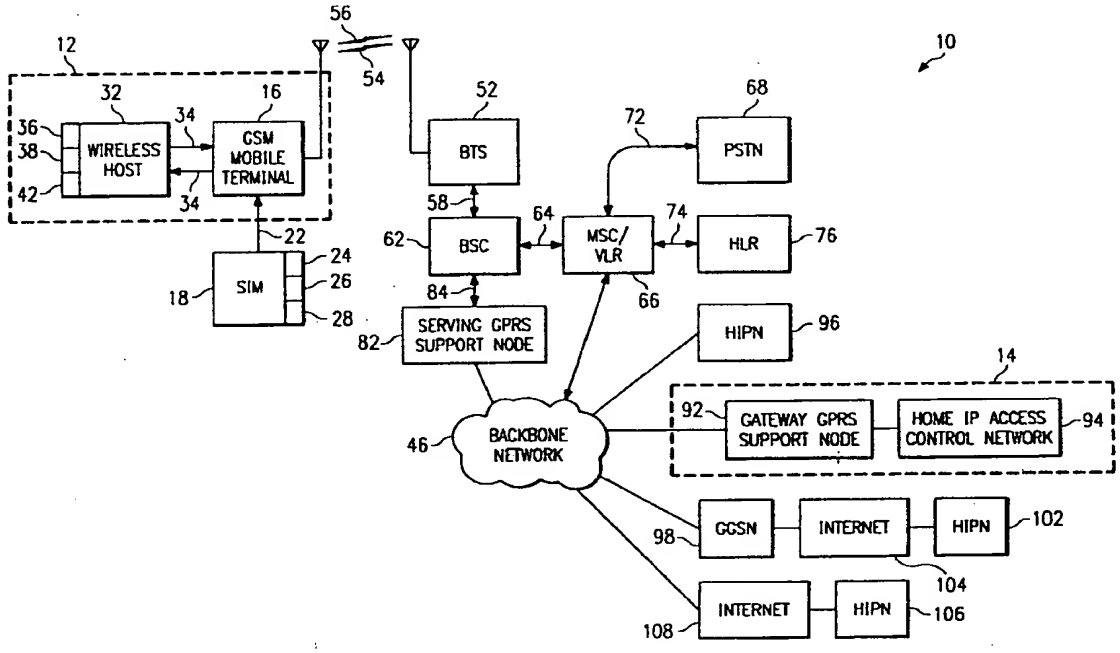
Primary Examiner—Ajit Patel

Attorney, Agent, or Firm—Jenkens & Gilchrist, P.C.

[57] **ABSTRACT**

A method, and associated apparatus, for accessing a private IP network with a wireless host by way of a wireless access network. Once authenticated and permitted access to the private IP network, the wireless host becomes a virtual host of the private IP network. A wireless host identifier (WHI) is used to identify the wireless host. Permission to communicate by way of wireless access network is confirmed by an authentication procedure. The WHI is thereafter provided to the private IP network. If the WHI is of a selected value, permission to access the private IP network is granted. An IP address used to address data to the wireless host is allocated by the private IP network once access to the private IP network is granted.

24 Claims, 2 Drawing Sheets



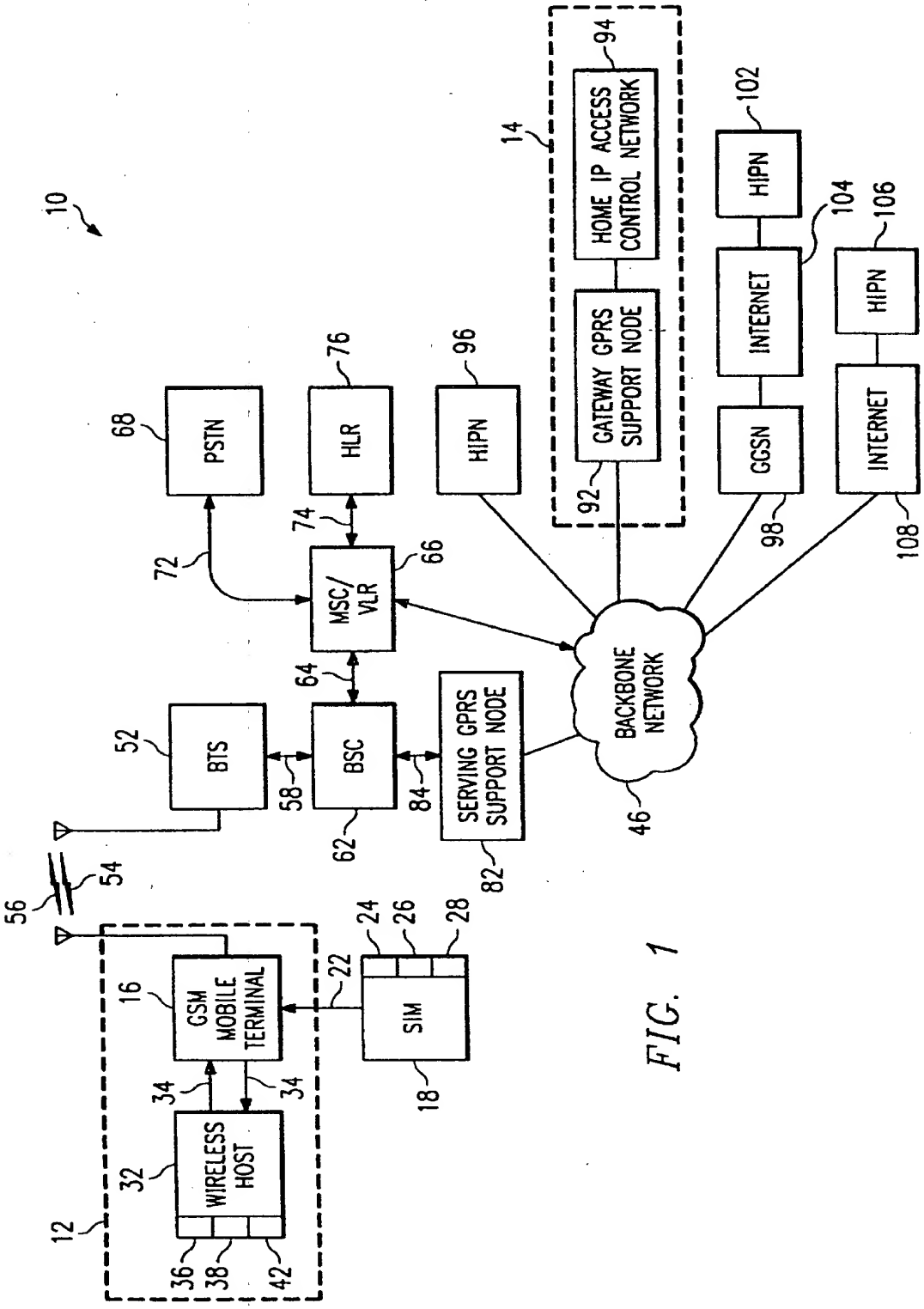

10
12
14
16
18
22
24
26
28
32
34
36
38
42
46
52
54
56
58
62
64
66
68
72
74
76
82
84
92
94
96
98
102
104
106
108
WIRELESS HOST
GSM MOBILE TERMINAL
SIM
BTS
BSC
MSC/ VLR
HLR
PSTN
SERVING GPRS SUPPORT NODE
BACKBONE NETWORK
HOME IP ACCESS CONTROL NETWORK
GATEWAY GPRS SUPPORT NODE
HIPN
GGSN
INTERNET
HIPN
INTERNET
HIPN

FIG. 1

FIG. 2

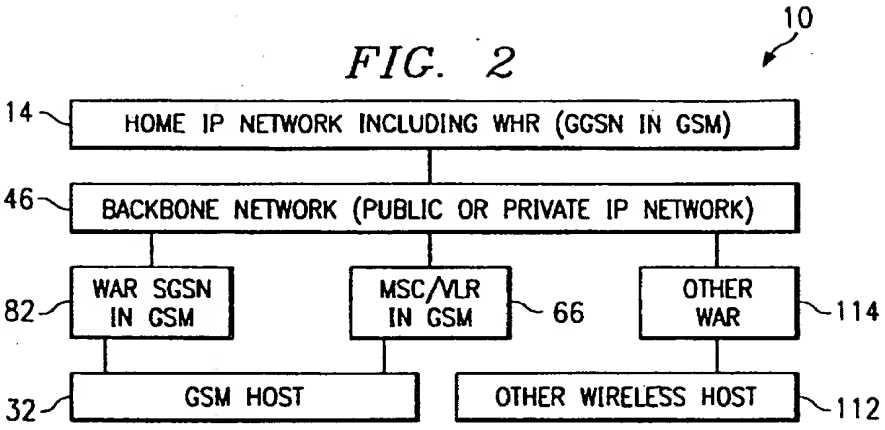


FIG. 3

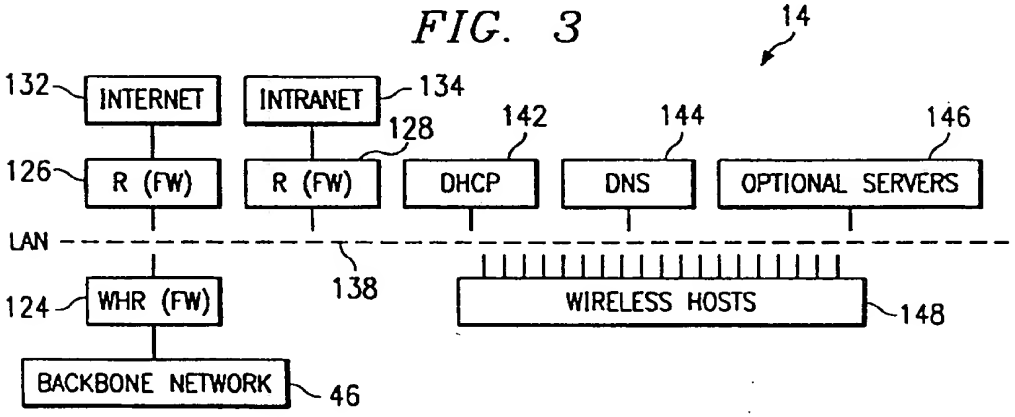
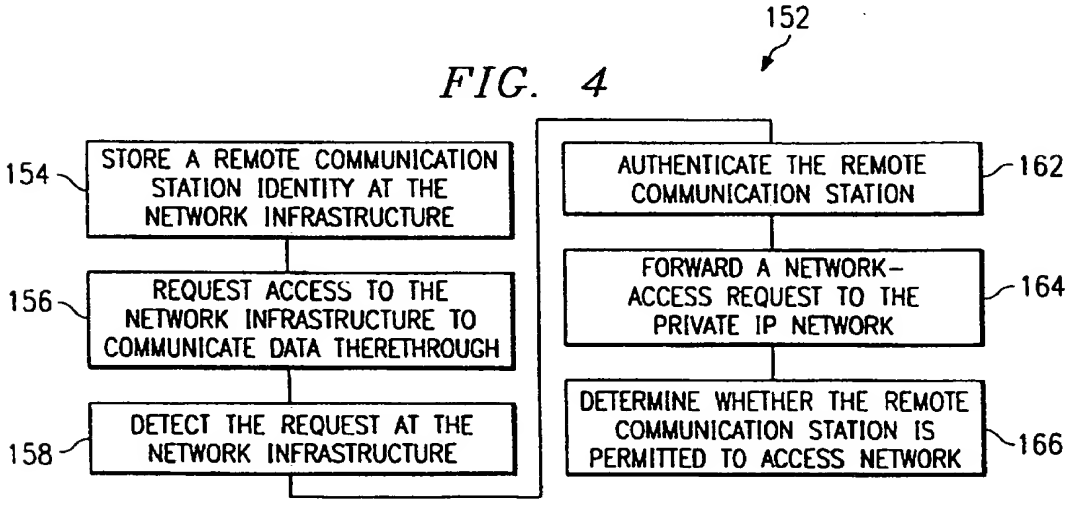


FIG. 4



SECURE ACCESS METHOD, AND ASSOCIATED APPARATUS, FOR ACCESSING A PRIVATE IP NETWORK

The present invention relates generally to communications between a wireless host and a network-located device. More particularly, the present invention relates to a method, and associated apparatus, for permitting the wireless host access to a private data communication network, such as a private IP network.

In an embodiment in which the private data communication network is formed of a private IP network, the private IP network is coupled to a wireless access network formed of the network infrastructure of a radio communication system, such as a cellular communication system. Once the wireless host is permitted access to the private IP network, an IP address is assigned to the wireless host by the private IP network. Information accessed at the private IP network is addressed to the wireless host using the IP address assigned by the private IP network.

A request by the wireless host to access the private IP network by the wireless host is transmitted first to the wireless access network. An authentication procedure is performed to confirm that the wireless host is permitted to communicate by way of the wireless access network. If the wireless host is authenticated, a wireless host identity (WHI), which identifies the wireless host is forwarded to the private IP network. The wireless host is permitted to access the private IP network if the WHI identifies a wireless host permitted to access the private IP network. The private IP network then allocates an IP address to the wireless host. The IP address is used to address data to the wireless host.

A simple and efficient manner by which to access a private IP, or other data communication, network is provided. A WHI is used to identify the wireless host in the wireless access network and at the private IP network. When the WHI is stored at the wireless access network, and does not have to be sent to the wireless access network infrastructure over an air interface. And, if the wireless host is permitted to access the private IP network, an IP address is assigned to the wireless host by the private IP network. The IP address can be dynamically allocated to the wireless host, and a separate IP address need not be permanently allocated to the wireless host.

BACKGROUND OF THE INVENTION

Advancements in communication technologies have permitted significant improvements in the manners by which data can be communicated between a sending and a receiving station.

For instance, in radio communications, advancements in digital communication techniques has permitted the introduction of, and popularization of, new types of communication systems. For example, cellular communication systems which utilize digital communication technologies have been installed in many areas and are widely utilized.

Advancements in communication technologies have also facilitated the decentralization of computer systems. Processing devices can be distributed at separate locations and connected together by network connections. Network connections between distributed processing devices and communications therebetween have precipitated, for instance, the advent of and wide availability of IP networks, such as the Internet. Other private data communication networks have similarly been formed.

The advancements in communication technologies have also permitted the merging of radio and network-connected

communication systems. For instance, it is possible for a terminal device, such as a portable computer, to be coupled by way of a radio link to network infrastructure of a radio communication system and, in turn, by way of a network connection to an Internet-connected, network device. The terminal device forms a wireless host to the Internet-connected network device as a physical, such as a hard-wired, link is not formed with the terminal device.

A private IP network is formed of a group of network devices, connected together by way of network connections, but to which access to the network is limited. Increasing numbers of private IP networks are being created and access thereto by a wireless host is increasingly demanded. Increasing numbers of other data communication networks are being created and access thereto by a wireless host is increasingly demanded.

Because of the limited-access nature of a private network, there is a need to insure that the wireless host is authorized to access the private network. And, if the wireless host is authorized to access the private network, there is a corresponding need to insure that the wireless host properly receives an acceptable level of access to the private network. That is to say, the wireless host should be treated as a virtual host, given the level of access to the private network as that given to a host physically coupled to such network.

Because the coupling of a wireless host to a network device of a private data communication network includes a radio link, the wireless host must be identified by an address so that data can be communicated thereto. In some existing communication systems in which a wireless host is able to communicate with a network device, the address of the wireless host is dynamically allocated. That is to say, e.g., in an embodiment in which the private data communication network is formed of a private IP network, rather than assigning a permanent IP address to the wireless host, a temporary IP address is assigned to the host when data is to be communicated to the wireless host. IPv6 dynamic IP address allocation is exemplary of an allocation method by which dynamically to allocate IP addresses to wireless hosts. In such method, to provide a fixed identity for the wireless host, a DNS (Domain Name System) name is allocated. A DNS name is a symbolic name provided for wireless hosts and other devices connected to an IP network.

One manner by which a wireless host can access a private IP network is to utilize a dial-out connection from the wireless host to the private IP network. Once a switched connection is formed, the wireless host is identified with a password.

Another manner by which a wireless host is sometimes able to access the private IP network is through the use of an authenticated tunnel. The wireless host is connected to the private IP network by way of the authenticated tunnel, and the wireless host is authenticated at the private IP network with an identity and a password. Such a tunneling method is sometimes referred to as "layer two tunneling." A PPTP system developed by MicroSoft Corporation, an L2F system developed by Sysco Systems, and an L2TP system developed by IETF are related to tunneling PPP.

The existing manners by which a wireless host accesses a private IP, or other data communication, network requires significant amounts of protocol overhead. As in any bandwidth-limited communication system, protocol overhead is width-consumptive.

When the wireless host accesses the private network by way of the network infrastructure of a cellular communication system, portions of the network infrastructure function

as a wireless access network. When, e.g., the private data communication network forms a private IP network, two IP addresses are required to permit communications between the wireless host and the private IP network. A first IP address is required at the wireless access network formed of the portion of the network infrastructure, and a second IP address is required at the private IP network. Thereby, the wireless host is required to belong to two networks, i.e., the access IP network and the private IP network.

As a result, two IP addresses must be allocated to the wireless host. If DNS is used in the two networks, it would also be necessary to allocate DNS names in both networks.

The layer two tunneling method requires formation of a protocol stack having three extra layers, the PPP layer, a layer two tunneling layer, and a basic IP layer. The protocol overhead resulting from such additional protocol layers is bandwidth-consumptive. Such a requirement is generally undesirable in a bandwidth-limited system.

Some wireless hosts are additionally capable of communicating packet data by way of circuit-switched as well as packet-switched connections. A GSM (Global System for Mobile communications) cellular communication system is exemplary of a cellular communication system which permits wireless hosts operable therein to communicate packet data by way of packet-switched and also circuit-switched connections. It would be advantageous to provide a manner by which to permit access of the wireless host to a private IP, or other data communication, network using the same access procedure irrespective of the type of data which is to be communicated therebetween.

In conventional manners by which to provide access of a wireless host to, e.g., a private IP network, dial-up connections are made directly to the private IP network. That connection may be made, for instance, to a remote access server of the private IP network. Telephonic charges associated with the dial-up connection can be significant. For instance, a long-distance toll might be charged to form the dial-up connection if an inter-LATA switched connection, or the like, is required between the network infrastructure of the cellular communication system and the private IP network. It would, of course, be desirable for the wireless host instead to be able to access a wireless access network as close as possible to the location at which the wireless host is positioned and thereafter to utilize IP transmission between the wireless access network and the private IP network.

A manner by which better to permit access of a wireless host to access a private data communication network to communicate packet data therebetween would be advantageous.

It is in light of this background information related to access of a wireless host and to a private IP network that the significant improvements of the present invention have evolved.

SUMMARY OF THE INVENTION

The present invention advantageously provides a method, and associated apparatus, for permitting a wireless host access to a private data communication network, such as a private IP network. The present invention further advantageously provides a method, and associated apparatus, once access is granted to the private network, for dynamically allocating a temporary address to the wireless host. The dynamically-allocated address is used to address data which is to be communicated to the wireless host.

In one aspect of the present invention, the wireless host is coupled by way of an air interface to the network infrastructure of a PLMN (Public Land Mobile Network), such as a GSM network. The PLMN is, in turn, coupled to a private IP network. The network infrastructure forms thereby a wireless access network. When the wireless host requests access to the private IP network, communications are first authenticated at the wireless access network formed of the network infrastructure of the PLMN. An authentication procedure is performed to confirm that communications are permitted by way of the wireless access network. If the authentication procedure confirms that such communications are permitted, a wireless host identity (WHI), previously stored at the wireless access network and which identifies the wireless host, is forwarded to the private IP network. The private IP network permits access to the wireless host if the wireless host identity provided thereto corresponds with the identity of a wireless host permitted to access the private IP network. An IP address is allocated to the wireless host by the private IP network. Such IP address is used to address data communicated to the wireless host. The IP address can be a dynamically-allocated address, used for a selected period to identify temporarily the wireless host.

Thereby, the wireless host is not required to have a separate IP identity to access a wireless access network. Instead, a wireless host identity stored at the wireless access network formed of the infrastructure of the PLMN is used to identify the wireless host at the private IP network. The wireless host identity may be provided e.g., as subscription data in the wireless access network. The wireless host identity is selected, e.g., by the operator of the private IP network, and the wireless host identity is provided to, and stored at, the network infrastructure of the PLMN pursuant to agreement between the operator of the private IP network and the operator of the PLMN.

Once provided access to the private IP network, an IP address for the wireless host is provided by the private IP network and not the PLMN. The wireless host is permitted to become a virtual host of the private IP network thus ensuring that the user and host environment, including security and firewalls, of the private IP network, shall similarly apply to the wireless host. IP tunneling is used between the PLMN and the private IP network. The IP tunnel can be secured by either by an authentication process or by arranging for secure transmissions by arrangements between the operators of the PLMN and the private IP network. The tunnel authentication keys maybe stored together with the WHI at the HLR, the SIM card, or at the wireless host to provide secure transmission of the wireless host identity as well as other data. The tunneling, however, does not extend to the air interface. Instead, air-interface-specific, transmission protocols are used to communicate datagrams between the wireless host and the network infrastructure of the PLMN.

In these and other aspects, therefore, a secured-access method, and associated apparatus for implementing the method, accesses a private data communication network by a remote communication station. Once provided access, data is communicated between the private data communication network and the remote communication station. The private data communication network is coupled to the network infrastructure of the radio communication system. A remote communication station identity is stored at the network infrastructure of the radio communication system. A registration request is generated by the remote communication station for requesting registration of the remote communication station to access the network infrastructure to permit the communication of data therethrough. The registration

request is detected at the network infrastructure. The remote communication station is authenticated to confirm authorization of the remote communication station to communicate by way of the network infrastructure. A network-access request is forwarded to the private data communication network if the remote communication station is authenticated wherein the remote communication station is identified by the remote communication station identity. A determination is made, responsive to the network-access request, whether the remote communication station is permitted to access the private data communication network. And, the remote communication station is permitted to access the private data communication network if the remote communication station is determined to be permitted to access the private network. Subsequent to grant of permission to access the private data communication network, an address, such as a temporary address, can be assigned to the wireless host.

A more complete appreciation of the present invention and the scope thereof can be obtained from the accompanying drawings which are briefly summarized below, the following detailed description of the presently-preferred embodiments of the invention, and the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** illustrates a functional block diagram of a communication system in which an embodiment of the present invention is operable.

FIG. **2** illustrates a logical, functional block diagram illustrating the routing of data communicated between a wireless host and a private IP network.

FIG. **3** illustrates a functional block diagram of a private IP network which includes an embodiment of the present invention for allocating an address by which to address data communicated to a wireless host.

FIG. **4** illustrates a logical flow diagram illustrating the method steps of the method of an embodiment of the present invention.

DETAILED DESCRIPTION

Referring first to FIG. **1**, a communication system, shown generally at **10**, permits the communication of data between a remote communication station **12** and a private IP network **14**. The private IP network **14** here forms a private intranet to which access is selectively permitted. When the remote communication station **12** is permitted access to the private IP network **14**, data can be communicated therebetween. In one embodiment, packet data is communicated between the remote communication station **12** and the private IP network **14**. While a private IP network is shown in the exemplary embodiment illustrated in the figure, in other embodiments, access to other types of private data communication networks can analogously be effectuated through operation of an embodiment of the present invention. Therefore, while the following description shall be described with respect to a private IP network **14**, it should be understood that the present invention is also operable to permit access to other data communication networks.

In the exemplary embodiment illustrated in the figure, the communication system **10** is formed of a GSM (Global System for Mobile communications) cellular communication system of which the network infrastructure thereof forms a wireless access network to which the private IP network **14** is coupled. In other embodiments, the communication system **10** is alternately formed of other structure.

The radio communication station **10** includes a radio transceiver, here a GSM mobile terminal **16**. The mobile terminal **16** includes a SIM (Subscriber Identity Module) card **18** which is inserted into, or is otherwise connected, here indicated by the lines **22**, to the mobile terminal **16**.

The SIM card **18** includes a storage location **24** for storing authentication information, in conventional manner. The SIM card **18** further includes a storage location **26** for storing the address of the private IP network **14**. In one embodiment of the present invention, the SIM card further includes a storage location **28** for storing a WHI (Wireless Host Identifier). Other subscriber data can additionally be stored at other storage locations of the SIM card **18**.

The mobile terminal **16** is coupled to a wireless host **32**, here by way of lines **34**. The wireless **32**, in one embodiment, forms a portable computer capable of receiving data communicated thereto by a network device of the private IP network **14**. The wireless host **32** may alternately be coupled to the mobile terminal **16** by a contactless coupler, e.g., an infrared coupler. In one embodiment of the present invention, the wireless host **32** includes storage locations **36**, **38**, and **42** for storing data similar to that stored at the storage locations **24**, **26**, and **28**. Namely, in such an embodiment, authentication information, the address of the private IP address **14**, and the value of the WHI are stored at the storage locations **36–42**, respectively. In the exemplary embodiment illustrated in the figure, such information is redundantly stored at the storage locations of both the SIM card **18** and the wireless host **32**. In other embodiments, merely the authentication information is stored at one of the storage locations **24** or **36**.

The network infrastructure of the communication system **10** forms a wireless access network which is coupled to the private IP network **14** by way of a backbone network **46**. The wireless access network formed of the network infrastructure of the GSM system is here shown to include a BTS (Base Transceiver Station) **52**. The BTS **52** is operable to generate downlink signals **54** and to receive uplink signals **56** upon an air interface formed of radio links between the remote communication station and the BTS **52**.

In the embodiment in which portions of the communication system **10** are formed of a structure of a GSM communication system, such structure, as well as the air interface formed between the remote communication station **12** and the BTS **52** are defined by the specification standards of the GSM system.

Groups of BTSs, of which a single BTS **52** is shown in the figure, are coupled by way of lines **58** to a BSC (Base Station Controller) **62**. The BSC **62** is operable, inter alia, to control operation of the BTSs coupled thereto. The BSC **62** is further coupled, here by way of lines **64**, to a MSC/VLR (Mobile Switching Center/Visited Location Register) **66**. The MSC/VLR **66** is operable in conventional manner to form appropriate connections to form a communication path between the BSC **62** and a PSTN (Public-Switched Telephonic Network) **68** by way of lines **72**.

The MSC/VLR **66** is further coupled, by way of lines **74**, to an HLR (Home Location Register) **76**. The HLR **76** includes an authentication center (not separately shown) at which, inter alia, an IMSI (International Mobile Subscriber Identity) and a value of a pseudo-random number are stored. Such values are utilized during authentication procedures used to confirm the authenticity of the remote communication station.

In an embodiment of the present invention, a value of WHI associated with the wireless host **32** is also stored at the HLR **76**. And, in another embodiment of the present invention, an address associated with the private IP network **14** is also stored at the HLR **76**.

Both the BSC **62** and the HLR **76** are further coupled to a SGSN (Serving GPRS Support Node) **82**. The BSC **62** is coupled to the SGSN **82** by way of lines **84**. And, the HLR **76** is coupled to the SGSN **82** by way of lines **86**. The SGSN **82** is further coupled to the backbone network **46** by way of lines **88**. Thereby, the SGSN **82** is coupled to the private IP network **14**.

The private IP network **14** here forms an HIPN (Home Intelligent Peripheral Network), here shown to include a GGSN (Gateway GPRS Support Node) **92** and a home IP access control network **94**. Additional details of the HIPN forming the private IP network **14** shall be described below with respect to FIG. **3**.

The backbone network **46** is further coupled to additional IP networks, such as the IP network **96**.

The backbone network **46** is further shown to be coupled by way of a GGSN **98** to another IP network forming another HIPN, here HIPN **102**, by way of an Internet connection **104**. And, the backbone network **46** is also coupled to an additional private IP network, forming an additional HIPN **106** by way of an Internet connection **108**. Such additional HIPNs **96**, **102**, and **106** are exemplary and are shown to illustrate manners by which private IP networks can be coupled to a wireless access network such as the network infrastructure of the GSM system shown in the figure.

During operation, when an operator of the wireless host **32** desires to access the private IP network **14**, appropriate commands are generated at the wireless host to initiate a request for access to the private IP network **14**. Signals indicative of such request are provided to the mobile terminal **16**, and the mobile terminal **16** generates a request over the air interface as an uplink signal **56** communicated to the BTS **52**. In a GSM communication system, an attach procedure is initiated. The BTS **52** forwards the request through the BSC **62** to the MSC/VLR **66**.

The IMSI and pseudo-random number of values are retrieved from the HLR **76** and an authentication procedure is carried out. While details of the authentication procedure carried out in a GSM communication system can be found in the specification standards of the GSM system, in general, the authentication procedure authenticates, i.e., confirms, that the mobile terminal **16** is permitted to communicate by way of the network infrastructure forming the wireless access network. Once the authentication procedure is successfully completed, i.e., the mobile terminal **16** is confirmed to be an authentic terminal which is permitted to communicate by way of the wireless access network formed of the network infrastructure, a value of the WHI associated with the wireless host is forwarded to the private IP network **14**.

In one embodiment, when the WHI is stored at the HLR **76**, the value stored thereat is provided by way of the line **86** to the SGSN **82**, through the backbone **46** and to the private IP network **14**. The WHI stored at the HLR is forwarded to the SGSN **82** if the authentication procedure confirms the authenticity of the mobile terminal **16**. Thereby, the value of the WHI is authenticated by the authentication procedure performed by the wireless access network. Storage of the WHI at the HLR **76**, or at another portion of the wireless access network, requires an agreement between an operator of the private IP network **14** and the operator of the wireless access network for the secure storage of the value of the WHI at the wireless access network. A separate IP address or DNS (Domain Name Service) name is provided only at the private IP network **14**, and not elsewhere. Thereby, because the IP address and DNS name is provided at the private IP network, the wireless host **32**, when permitted access to the private IP network, becomes a virtual host of the network **14**. The user and host environment of the network **14**, including security and firewalls of the network apply also to the wireless host **32**.

Access of the wireless host **32** to others of the networks, such as the HIPNs **96**, **102**, and **106**, can analogously be effectuated.

In one embodiment, authenticated IP tunneling is also performed between the SGSN **82** and the GGSN **92** over the backbone network **46** to ensure secure transmission of the WHI, and other data, between the private IP network **14** and the wireless access network formed of the network infrastructure. Such authenticated tunneling is performed as the backbone network **46** might be shared by many different operators and security of the backbone can not be assured. For instance, if the HIPN **106** is to be accessed, data is routed by way of a public Internet **108**. The authenticated IP tunneling is performed to authenticate traffic, i.e., communication of data, between the SGSN **82** and the GGSN **92**. Authenticating the traffic routed over the backbone ensures the validity of the value of the WHI when the value is received at the GGSN **92**. When, e.g., the HIPN **102** is instead to be accessed, the transmission over the Internet **104** similarly is authenticated by an authentication procedure.

In one embodiment, the GGSN **92** includes an access control mechanism to ensure that only values of wanted-WHIs are permitted to gain access to the private IP network. A list of wanted-WHIs is stored at the access control mechanism of the GGSN **92**. And, a WHI authentication procedure may further be performed to increase further the security level and minimize the possibility of erroneous access to the private IP network responsive to WHI administration mistakes. While not separately shown in FIG. **1**, the SGSN **82** and the GGSN **92** are protected by firewalls positioned towards the backbone network **46**.

Within the private IP network **14**, standard, HIPN security procedures, such as e.g., firewalls and passwords, are used. Thereby, the wireless host **32**, once access to the private IP network is permitted, is provided with the same environment and security level as any other host connected directly to the network **14**.

FIG. **2** illustrates the logical arrangement of portions of the communication system **10** shown in FIG. **1**. Again, during operation of an embodiment of the present invention, a wireless host, here the wireless host **32**, is selectively permitted to access the private IP network, here again shown to form an HIPN, **14**.

When the wireless host **32** is to gain access to the private IP network **14**, the mobile terminal **16** generates an attach request to attach to the wireless access network formed of the network infrastructure of the GSM system. The attachment procedure is performed pursuant to the SGSN **82** when using packet-switched circuit connections. And, the attach procedure is performed pursuant to the MSC/VLR **66** when circuit-switched circuit connections are used.

During the attach procedure, the values of the IMSI, the WHI, and other associated subscriber data is downloaded from the HLR **76** to the appropriate one of the MSC/VLR **66** and SGSN **82**. The other appropriate subscriber data includes the address of the private IP network **14**. Addresses of additional private IP networks, such as the HIPN **96**, **102**, and **106** (shown in FIG. **1**) may also be downloaded to permit alternate, or second-choice access to an alternate IP network. The HIPN address identifying the private IP network **14**, in one embodiment, is the address of the GGSN, such as the GGSN **92** of the private IP network **14**.

Thereafter, the mobile terminal **16** generates a "PDP routing context activation request" to the SGSN **82** or an access to the MSC/VLR **66**, as appropriate. The access to the MSC/VLR **66** is performed, for instance, by placing a call originated at the mobile terminal. Alternatively, standardization of additional protocol over the air interface to explicitly indicate that the MSC/VLR should be accessed can be made.

Pursuant to the activation request to the SGSN **82** or the access to the MSC/VLR **66**, an indication of which HIPN is to be accessed is further provided to the SGSN or MSC/VLR, as appropriate. The mobile terminal **16** indicates, for instance, that the private IP network identified by the HIPN address stored at the HLR is the address of the private IP network which is to be accessed. Alternatively, the mobile terminal **16** can itself provide the address of the private IP network which is to be accessed. Or, a default address can be used to identify the private IP network which is to be accessed.

The appropriate one of the SGSN **82** and the MSC/VLR **66** analyzes the value of the IMSI provided thereto and determines the address of the default, private IP network if the address is not otherwise provided thereto.

The appropriate one of the SGSN **82** and MSC/VLR **66** generates a "create PDP context" command which is forwarded, by way of the backbone network **46** to the GGSN **92**, when the private IP network **14** is to be accessed, or another GGSN when another network is, instead, to be accessed. The "create PDP context" command includes the WHI of the wireless host, and such value is used as the host identity at the HIPN forming the private IP network **14**.

FIG. **2** further illustrates a wireless host **112** which is connectable to another WAR (Wireless Access Router) **114** by way of a radio link. And, the WAR **114** is coupled to the backbone network **46**. The wireless host **112** is exemplary of another device to which access might be permitted to the IP network **14**.

FIG. **3** illustrates a logical model of the private IP network **14**, formed of an HIPN, shown previously in FIGS. **1** and **2**. The HIPN formed of the network **14** provides services and a user environment including the following: a DHCP (Dynamic Host Configuration Profile) service, a DNS (Domain Name Service) service, a news service, a mail service, a log-in service, an NTP service, a WWW (World Wide Web) service, other application servers, connection to an Internet, connections to intranets, connection to a backbone network, and firewalls at each interface to which connection is made to another network.

Access to a private IP network by the wireless host **32** provides vertical services and access to the home organization of a mobile terminal. In such a scenario, the private IP network is part of the private network of a service provider. A public IP network provides public Internet services. If, instead, a public IP network is accessed, the public IP network is situated at an Internet service provider at either a home or a visited, PLMN (Public Land Mobile Network), provided by its operator or a dedicated Internet service provider.

With reference, then, to FIG. **3**, the HIPN forming the private IP network **14** is again shown to be coupled to the backbone network **46**. A WHR (Wireless Host Router) **124** which also functions as a firewall is coupled to the backbone network **46**. The WHR **124** is formed of a router having special support for selectively permitting a wireless host, such as the wireless host **32**, to become a virtual host of the network. The network **14** includes other routers, here routers **126** and **128**, which are connected to an Internet **132** and an intranet **134**, respectively. The routers **124–128** are connected by way of a local area network (LAN) **138** to which a DHCP (Dynamic Host Configuration Profile) device **142** and a DNS (Domain Name Service) device **144** are also coupled. Other, optional application servers, of which the server **146** is representative, are also shown in the figure, also connected to the LAN **138**. And, wireless hosts **148**, directly coupled to the private IP network **14** are further pictured in the figure in connection with the LAN **138**.

The DHCP **142** is operable to allocate addresses to wireless hosts, such as the wireless host **32**. A WHI value is used as a wireless host address at the DHCP **142**. The DNS **144** is operable to store names of the wireless hosts, such as the wireless host **32**. The value of the WHI is used as a primary name at the DNS **144**, and other secondary names can also be stored in conjunction with the WHI. Exemplary, DNS names include, for instance, WHI24450123456789@org.country; MSISDN467051234567@org. country; and myhost@org.country.

The value of the WHI can be advantageously utilized because such value is a secure, wireless-network-provided identity which unambiguously identifies the wireless subscription used at the wireless host. By storing the value of the WHI as subscriber data at the HLR **76** (shown in FIG. **1**), the value of the WHI is stored with an appropriate level of security. As the wireless host accessing the GSM network is authenticated prior to receiving permission to use the WHI stored thereat, no separate log-in is needed to access the private IP network **14**.

Transmission between the private IP network **14** and the wireless access router **124** must be secure. To ensure security of the transmission, the wireless host router **124** and the wireless access router forming a portion of the GSM, the wireless access network stores the address and authentication information about the respective routers between which communication is permitted. Such measures ensure that a WHI arriving at the wireless host router **124** is secure and correct. If necessary, transmission between the routers may be encrypted to provide greater assurances of data confidentiality and reliability. Optionally, an authentication procedure at the WHR **124** may be associated to the WHI, thus protecting the IP network from mistakes made in the WHI administration.

WHI and an authentication key may also be received from the wireless host **32**, and authentication procedures can additionally be performed at the private IP network prior to granting of permission of the wireless host **32** to access the private IP network.

Access attempts without a valid WHI are rejected by the GGSN. And, valid WHIs must be preconfigured in the WHR **124** as well as the DHCP **142** and DNS **144**. The DHCP **142** updates the DNS **144** with the allocated IP address used to address data to be communicated to the wireless host.

While the private IP network **14** shown in FIG. **3** illustrates only a single LAN **138**, the network can, instead, be implemented on several physical LANs or implemented on a single platform without a physical LAN. When WHRs analogous to the WHR **124** are present at several physical locations, each WHR is considered as a subnetwork (SHIPN) of the HIPN forming the private IP network. In such an arrangement, each SHIPN is able to communicate with another SHIPN by way of a backbone network.

FIG. **4** illustrates the method, shown generally at **152**, of an embodiment of the present invention. The method **152**

provides a secured-access method for accessing a private IP network by a remote communication station.

First, and as indicated by the block **154**, a remote communication station identity is stored at the network infrastructure forming a wireless access network of a radio communication system. The remote communication station identity is stored together with authentication data associated with the remote communication station.

Then, and as indicated by the block **156**, a request is generated by the remote communication station for requesting access to the network infrastructure to permit communication of data therethrough.

The request is detected, as indicated by the block **158**, at the network infrastructure. The remote communication station is authenticated, as indicated by the block **162**, to confirm authorization of the remote communication station to communicate by way of the network infrastructure.

Thereafter, an IP network-access request is forwarded to the private IP network, as indicated by the block **164**. Then, as indicated by the block **166**, a determination is made as to whether the remote communication station is permitted to access the private IP network.

And, the remote communication station is permitted to access the private IP network if the remote communication station is determined to be permitted to access the network.

During operation of an embodiment of the present invention permits a wireless host to become a virtual host of a private IP network. A wireless host identity (WIII) is used as a host identifier in the private IP network. The wireless host need only authenticate itself at the private IP network when no contract for safe storage exists between the operators of the wireless access network and the private IP network, regarding security of, e.g., identification information. An authentication procedure confirms the authenticity of the structure transmitting the access request. Bandwidth required over the air interface to generate the request to access the private IP network is advantageously also reduced when transferring IP packets over the air interface as only air-interface-specific protocols are used to transfer IP packets over the air interface.

The previous descriptions are of preferred examples for implementing the invention, and the scope of the invention should not necessarily be limited by this description. The scope of the present invention is defined by the following claims.

What is claimed is:

1. In a method for communicating data between a private data communication network and a remote communication station, the private data communication network coupled to network infrastructure of a radio communication system of which the remote communication station forms a portion, an improvement of a secured-access method of accessing the private data communication network by the remote communication station, said method comprising the steps of:

storing a remote communication station identity which identifies the remote communication station at the network infrastructure;

generating a request by the remote communication station to access the network infrastructure to permit communication of data therethrough;

detecting at the network infrastructure the request generated during said step of generating;

authenticating the remote communication station to confirm authorization of the remote communication station to communicate by way of the network infrastructure;

the remote communication station identity stored together with authentication data associated with the remote communication station;

forwarding a network-access request to the private data communication network if the remote communication station is authenticated during said step of authenticating, the remote communication station identified by the remote communication station identity stored during said step of storing;

determining, responsive to the network-access request forwarded during said step of forwarding, whether the remote communication station is permitted to access the private data communication network; and

permitting the remote communication station to access the private data communication network if the remote communication station is determined, during said step of determining, to be permitted to access the private data communication network.

2. In a method for communicating data between a private IP (Internet Protocol) network and a remote communication station, the private IP network coupled to network infrastructure of a radio communication system of which the remote communication station forms a portion, an improvement of a secured-access method of accessing the private IP network by the remote communication station, said method comprising the steps of:

storing a remote communication station identity which identifies the remote communication station at the network infrastructure;

generating a request by the remote communication station to access the network infrastructure to permit communication of data therethrough;

detecting at the network infrastructure the request generated during said step of generating;

authenticating the remote communication station to confirm authorization of the remote communication station to communicate by way of the network infrastructure;

the remote communication station identity stored together with authentication data associated with the remote communication station;

forwarding an IP network-access request to the private IP network if the remote communication station is authenticated during said step of authenticating, the remote communication station identified by the remote communication station identity stored during said step of storing;

determining, responsive to the IP network-access request forwarded during said step of forwarding, whether the remote communication station is permitted to access the private IP network; and

permitting the remote communication station to access the private IP network if the remote communication station is determined, during said step of determining, to be permitted to access the private IP network.

3. The method of claim **2** wherein the remote communication station comprises a wireless host coupled to a radio transceiver, the radio transceiver operable to communicate with the network infrastructure, and wherein said step of storing comprises storing a wireless host identity, the wireless host identity associated with the wireless host.

4. The method of claim **3** wherein the wireless host identity is stored at the wireless host.

5. The method of claim **4** wherein the wireless host identity is stored at the radio transceiver.

6. The method of claim **5** wherein the radio transceiver comprises a cellular mobile terminal operable in a cellular

communication system, the cellular mobile terminal having a memory card, and wherein the wireless host identity is stored at the memory card.

7. The method of claim 2 wherein the radio communication system comprises a cellular communication system, wherein the remote communication station comprises a wireless host coupled to a radio transceiver and wherein said step of generating the request comprises generating an attach request, the attach request for requesting attachment, by way of a radio link, of the radio transceiver with the network infrastructure of the cellular communication system by way of an air interface formed therebetween.

8. The method of claim 2 wherein the radio communication system comprises a cellular communication system, wherein the data communicated between the remote communication station and the private IP network comprises packet data, and wherein the request generated during said step of generating is provided to a router which routes packet data.

9. The method of claim 8 wherein the cellular communication system comprises a GSM communication system and wherein the router to which the request is provided comprises a SGSN (Servicing GPRS Support Node).

10. The method of claim 2 wherein the radio communication system comprises a cellular communication system, wherein the data communicated between the remote communication station and the private IP network comprises packet-switched data, and wherein the request generated during said step of generating is provided to a router by way of a circuit-switched circuit connection.

11. The method of claim 10 wherein the cellular communication system comprises a GSM communication system and wherein the router to which the request is provided comprises an MSC/VLR (Mobile Switching Center/Visited Location Register).

12. The method of claim 2 wherein said step of storing further comprises the step of storing a private IP network identity identifying the private IP network between which the data is communicated with the remote communication station.

13. In a method for communicating data between a private IP (Internet Protocol) network and a remote communication station, the private IP network coupled to network infrastructure of a radio communication system of which the remote communication station forms a portion, an improvement of a secured-access method of accessing the private IP network by the remote communication station, said method comprising the steps of:

storing a remote communication station identity which identifies the remote communication station at a storage location;

generating a request by the remote communication station to access the network infrastructure to permit communication of data therethrough;

detecting at the network infrastructure the request generated during said step of generating;

authenticating the remote communication station to confirm authorization of the remote communication station to communicate by way of the network infrastructure;

forwarding an IP network-access request to the private IP network if the remote communication station is authenticated during said step of authenticating, the remote communication station identified by the remote communication station identity stored during said step of storing;

determining, responsive to the IP network-access request forwarded during said step of forwarding, whether the remote communication station is permitted to access the private IP network; and

permitting the remote communication station to access the private IP network if the remote communication station is determined, during said step of determining, to be permitted to access the private IP network;

wherein said step of storing further comprises the step of storing a private IP network identity identifying the private IP network between which the data is communicated with the remote communication station; and

wherein the IP network-access request forwarded during said step of forwarding is forwarded to the private IP network identified by the private IP network identity stored during said step of storing the private IP network identity.

14. In a method for communicating data between a private IP (Internet Protocol) network and a remote communication station, the private IP network coupled to network infrastructure of a radio communication system of which the remote communication station forms a portion, an improvement of a secured-access method of accessing the private IP network by the remote communication station, said method comprising the steps of:

storing a remote communication station identity which identifies the remote communication station at a storage location;

generating a request by the remote communication station to access the network infrastructure to permit communication of data therethrough;

detecting at the network infrastructure the request generated during said step of generating;

authenticating the remote communication station to confirm authorization of the remote communication station to communicate by way of the network infrastructure;

forwarding an IP network-access request to the private IP network if the remote communication station is authenticated during said step of authenticating, the remote communication station identified by the remote communication station identity stored during said step of storing;

determining, responsive to the IP network-access request forwarded during said step of forwarding, whether the remote communication station is permitted to access the private IP network; and

permitting the remote communication station to access the private IP network if the remote communication station is determined, during said step of determining, to be permitted to access the private IP network;

wherein said step of storing further comprises the step of storing a private IP network identity identifying the private IP network between which the data is communicated with the remote communication station; and

wherein said step of generating further comprises the step of generating a wireless-host-provided, IP network identity, the wireless-host-provided, IP network identity identifying the private IP network between which the data is to be communicated with the remote communication station.

15. The method of claim 14 wherein said step of generating further comprises the step of generating a wireless-host-provided IP network identity, the wireless-host-provided IP network identity identifying the private IP network between which the data is to be communicated with the remote communication station; and

wherein the IP network-access request forwarded during said step of forwarding is forwarded to the private IP

network identified by the wireless-host-provided IP network identity generated during said step of generating.

16. The method of claim 2 wherein the remote communication station has associated therewith a default-IP network identity and wherein the IP network-access request forwarded during said step of forwarding is forwarded to the private IP network identified by the default-IP network identity.

17. The method of claim 2 wherein said step of determining further comprises the step of authenticating an access request to access the private IP network.

18. The method of claim 2 wherein said step of determining comprises the steps of:

storing at the private IP network a list of remote communication station identities which identify remote communication stations permitted to access the private IP network; and

comparing the remote communication station identity associated with the IP network-access request forwarded during said step of forwarding with the remote communication station identities stored upon the list.

19. The method of claim 18 comprising the further step of allocating an address to the remote communication station at the private IP network if the remote communication station is permitted access thereto, the address allocated to the remote communication station for addressing data communicated by the private IP network to the remote communication station.

20. The method of claim 19 wherein the address allocated during said step of allocating comprises a temporary address, the temporary address identifying the remote communication station for a selected period.

21. In a radio communication system having a wireless access network, a private data communication network coupled to the wireless access network, and a remote communication station operable selectively to communicate data with the private data communication network by way of the wireless access network, an improvement of apparatus for selectively permitting access to the private data communication network by the remote communication station, said apparatus comprising:

a storage element at the wireless access network for storing a remote communication station identity identifying the remote communication station;

a detector coupled to the wireless access network, said detector for detecting a request requesting access by the remote communication station to the wireless access network to permit communication of data therethrough;

an authenticator coupled to the wireless access network, said authenticator for confirming authorization of the remote communication station to communicate by way of the wireless access network;

the remote communication station identity stored together with authentication data associated with the remote communication station;

a network access requester coupled to said authenticator, said network access requestor operable responsive to authentication by said authenticator, said network access requester for generating a request to request access to the private data communication network by the remote communication station, the remote communication station identified in the request by the remote communication station identity stored in said storage element; and

a determiner associated with the private IP network, said determiner operable responsive to the request requested by said network access requester to determine whether to permit access by the remote communication station to the private data communication network.

22. The apparatus of claim 21 further comprising an address allocator associated with the private IP network, said address allocator for allocating an address to the remote communication station, the address allocated by said address allocator used to address data communicated to the remote communication station by the private IP network.

23. The apparatus of claim 22 wherein said address allocator comprises a dynamic allocator for dynamically allocating a temporary IP address, the temporary IP address used to address the data communicated to the remote communication station for a selected period.

24. The apparatus of claim 21 wherein said storage element further stores a private data communication address identifying the private data communication network.

* * * * *

US006301479B1

(12) **United States Patent**
Roobol et al.

(10) **Patent No.: US 6,301,479 B1**
(45) **Date of Patent: Oct. 9, 2001**

(54) **TECHNIQUE FOR PROVIDING A SECURE LINK IN A MOBILE COMMUNICATION SYSTEM**

(75) Inventors: **Christiaan Roobol**, Aachen (DE); **Mathias Johansson**, Sollentuna (SE); **Raul Söderstrom**, Kyrkslatt (FI); **Bela Rathonyi**, Malmö (SE); **Joachim Sachs**, Aachen (DE)

(73) Assignee: **Telefonaktiebolaget LM Ericsson**, Stockhom (SE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/349,899**

(22) Filed: **Jul. 8, 1999**

(51) **Int. Cl.**[7] **H04L 12/413**
(52) **U.S. Cl.** **455/436**; 455/410; 455/414
(58) **Field of Search** 455/436, 449, 455/414, 560, 410, 411

(56) **References Cited**

FOREIGN PATENT DOCUMENTS

WO 99/34635 7/1999 (WO) .

OTHER PUBLICATIONS

John Scourias; Overview of the GLobal System for Mobile Communications; 1996, 1997; 14 page; Website cenga.uwaterloo.ca/~jscouria/GSM/gsmreport.html.

Raj Jain; Wireless ATM—An Overview; 1997; 10 pages; Website cis.ohio-state.edu/~jain/cis788-97/wirelessatm/index.htm#rrc.

Peter Rysavy; Paper: General Packet Radio Service (GPRS); Sep. 30, 1998; 6 pages; Website pcsdata.com/paprysavy.htm.

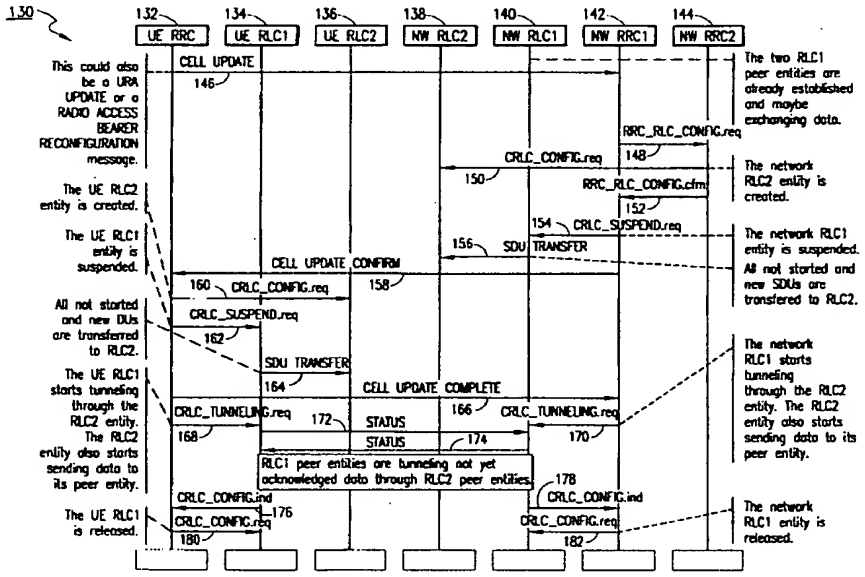
Nokia; Third Generation—personal, multimedia mobile communications; 1995–1998; 19 pages; Website nokia.com/3g/index.html.

Primary Examiner—Daniel Hunter
Assistant Examiner—Thuan T. Nguyen
(74) *Attorney, Agent, or Firm*—Jenkens & Gilchrist P.C.

(57) **ABSTRACT**

A technique for providing a secure link when transitioning between pairs of link layer protocol entities in a mobile communication system is disclosed. The first pair of link layer protocol entities includes a first transmitting link layer protocol entity and a first receiving link layer protocol entity. The second pair of link layer protocol entities includes a second transmitting link layer protocol entity and a second receiving link layer protocol entity. The technique is realized by first suspending data transmissions from the first transmitting link layer protocol entity to the first receiving link layer protocol entity, and then initiating data transmissions from the second transmitting link layer protocol entity to the second receiving link layer protocol entity. Unacknowledged segmented data in the first transmitting link layer protocol entity is then tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

40 Claims, 8 Drawing Sheets



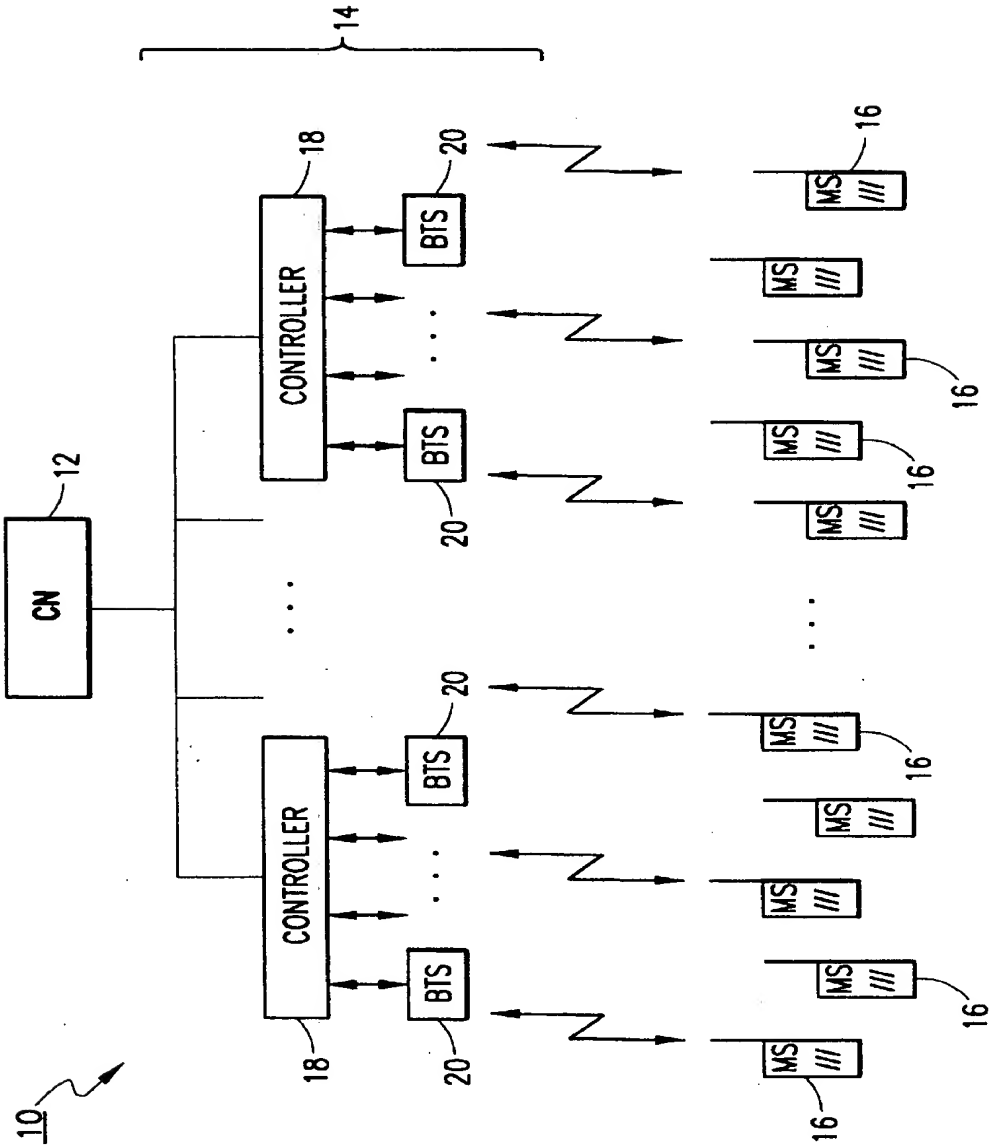


FIG. 1
(PRIOR ART)

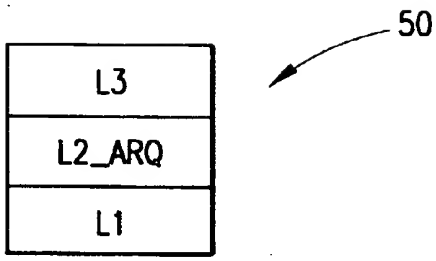

50
L3
L2_ARQ
L1

FIG. 2

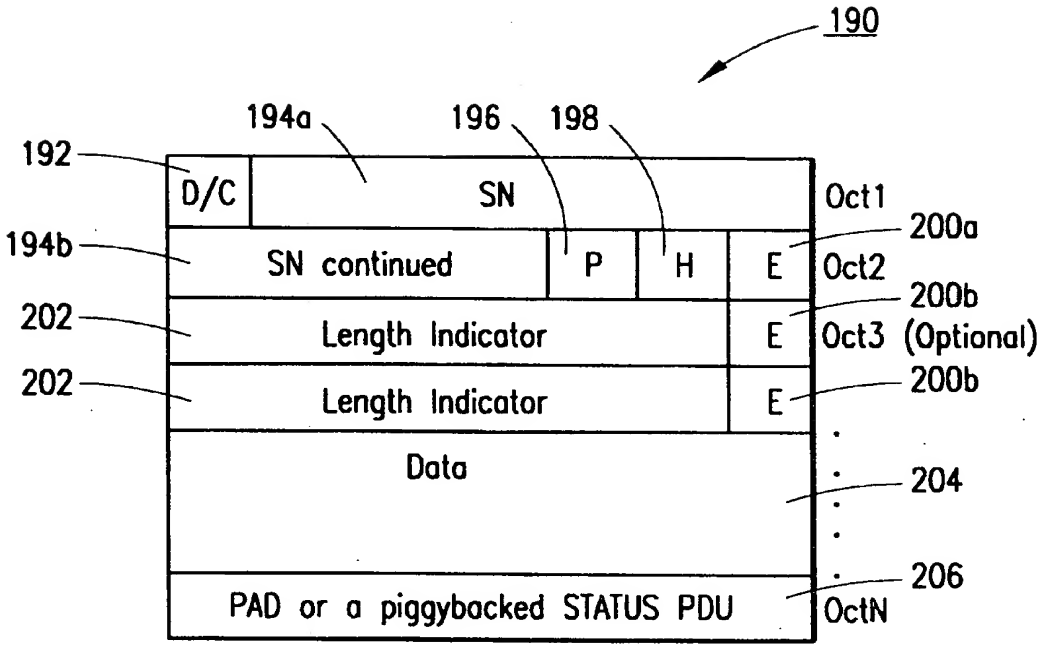

190
194a
196
198
192
D/C
SN
Oct1
200a
194b
SN continued
P
H
E
Oct2
200b
202
Length Indicator
E
Oct3 (Optional)
202
Length Indicator
E
200b
Data
204
206
PAD or a piggybacked STATUS PDU
OctN

FIG. 7

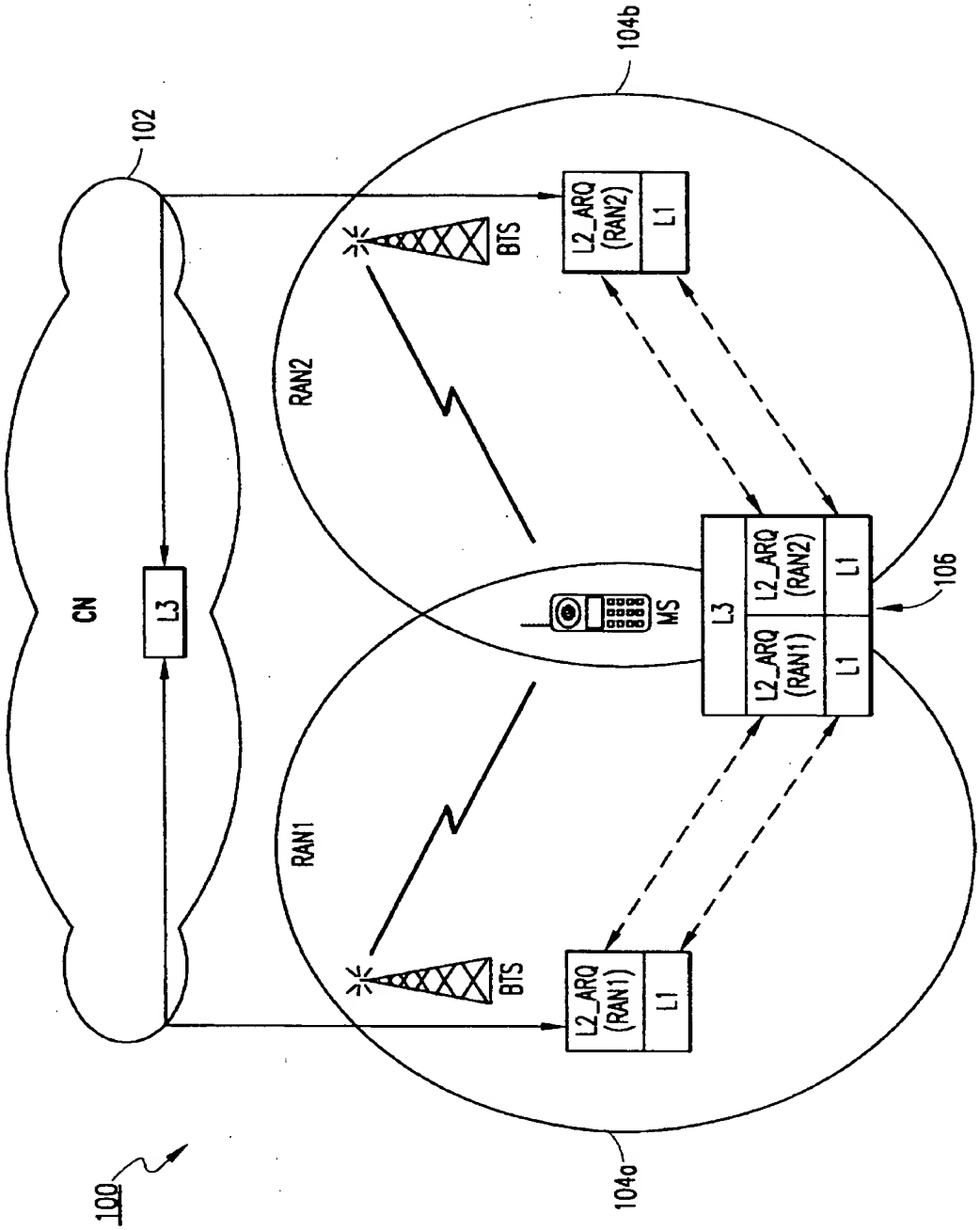

100
102
CN
L3
104b
RAN2
BTS
L2_ARQ (RAN2)
L1
MS
L3
L2_ARQ (RAN2)
L1
L2_ARQ (RAN1)
L1
106
RAN1
BTS
L2_ARQ (RAN1)
L1
104a

FIG. 3

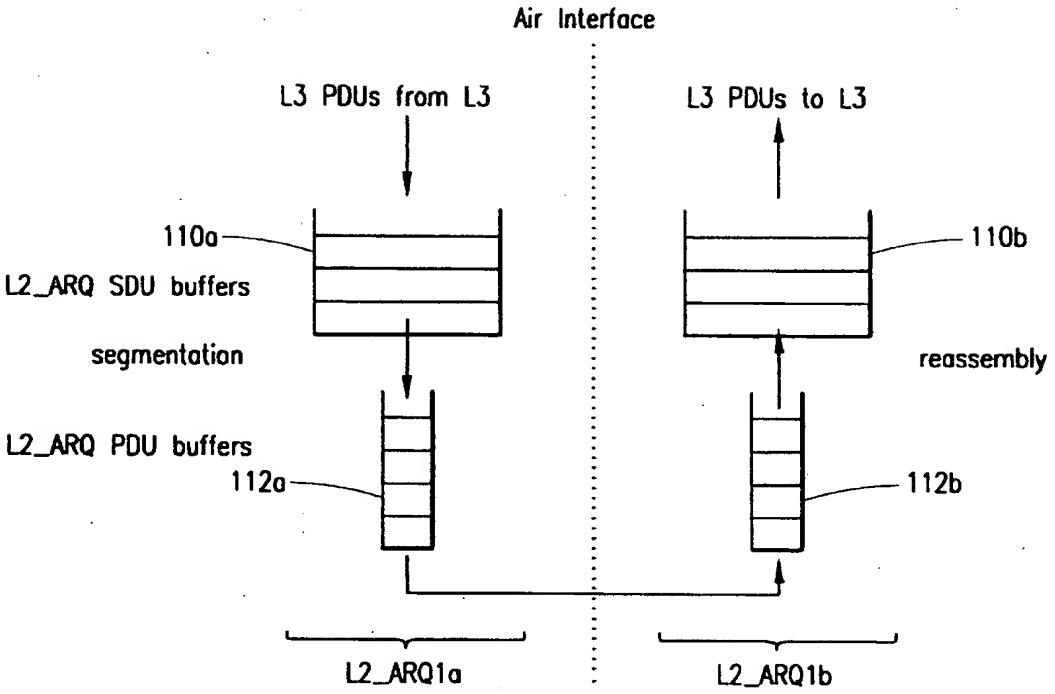

Air Interface
L3 PDUs from L3
L3 PDUs to L3
110a
L2_ARQ SDU buffers
110b
segmentation
reassembly
L2_ARQ PDU buffers
112a
112b
L2_ARQ1a
L2_ARQ1b

FIG. 4

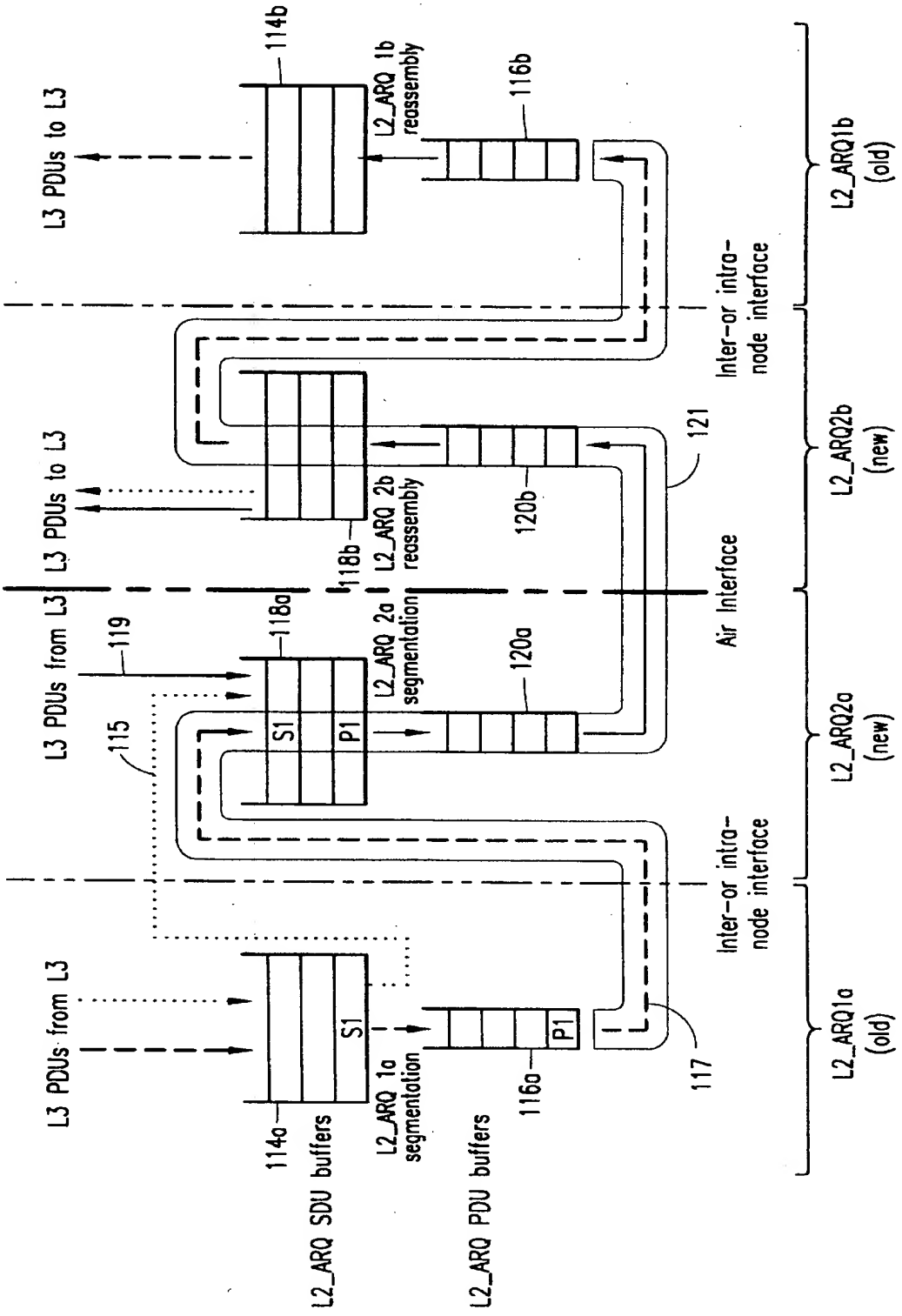

L3 PDUs to L3
L3 PDUs from L3
L2_ARQ SDU buffers
L2_ARQ PDU buffers
L2_ARQ 1a segmentation
L2_ARQ 2a segmentation
L2_ARQ 2b reassembly
L2_ARQ 1b reassembly
Air Interface
Inter-or intra-node interface
L2_ARQ1a (old)
L2_ARQ2a (new)
L2_ARQ2b (new)
L2_ARQ1b (old)
S1
P1
114a
116a
118a
120a
118b
120b
114b
116b
115
117
119
121

FIG. 5

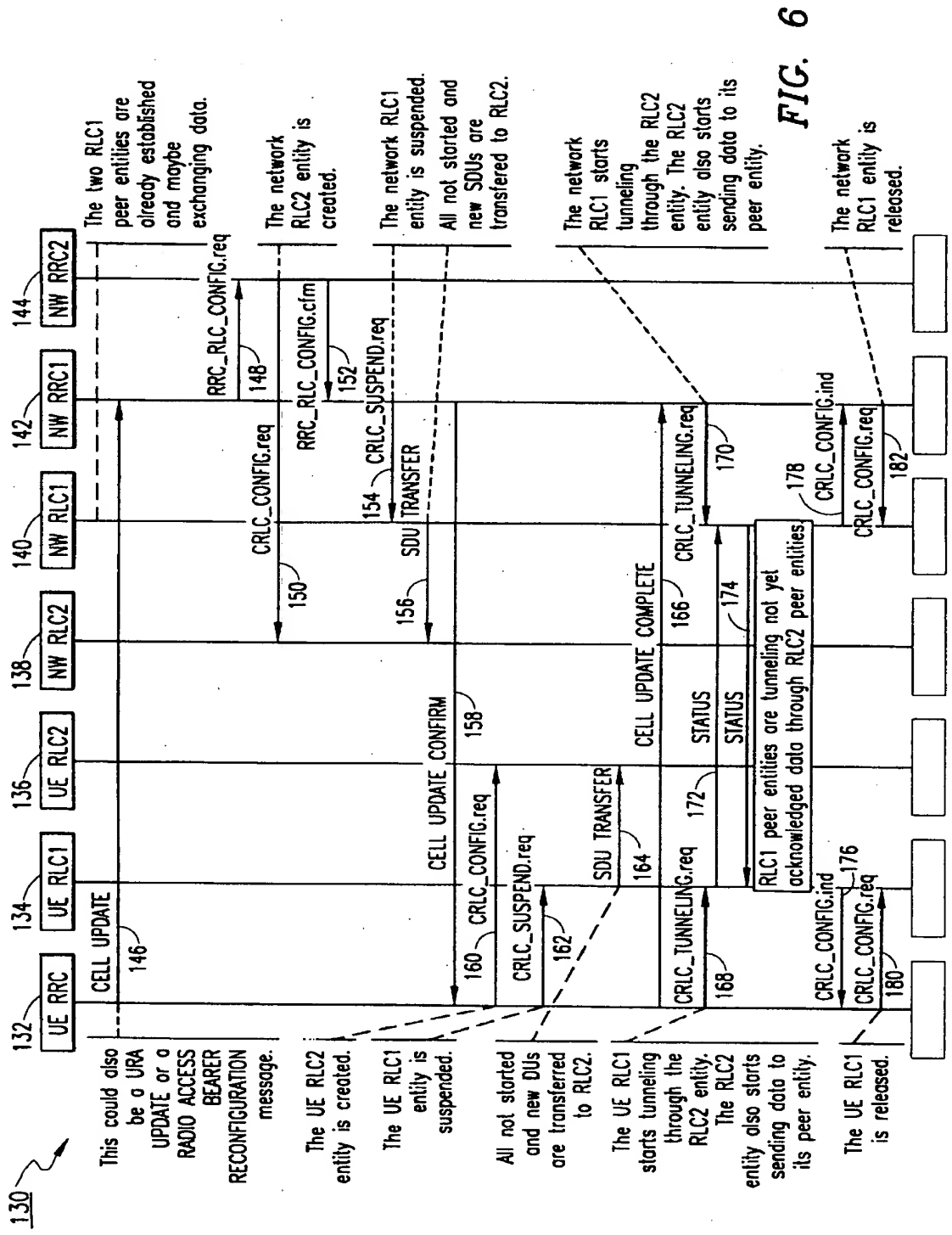

130
132 UE RRC
134 UE RLC1
136 UE RLC2
138 NW RLC2
140 NW RLC1
142 NW RRC1
144 NW RRC2
The two RLC1 peer entities are already established and maybe exchanging data.
CELL UPDATE 146
This could also be a URA UPDATE or a RADIO ACCESS BEARER RECONFIGURATION message.
RRC_RLC_CONFIG.req 148
The network RLC2 entity is created.
RRC_RLC_CONFIG.cfm 152
CRLC_CONFIG.req 150
The UE RLC2 entity is created.
CRLC_SUSPEND.req 154
SDU TRANSFER 156
The network RLC1 entity is suspended. All not started and new SDUs are transfered to RLC2.
The UE RLC1 entity is suspended.
CELL UPDATE_CONFIRM 158
CRLC_CONFIG.req 160
CRLC_SUSPEND.req 162
All not started and new DUs are transferred to RLC2.
SDU TRANSFER 164
CELL UPDATE COMPLETE 166
CRLC_TUNNELING.req 170
The network RLC1 starts tunneling through the RLC2 entity. The RLC2 entity also starts sending data to its peer entity.
The UE RLC1 starts tunneling through the RLC2 entity. The RLC2 entity also starts sending data to its peer entity.
CRLC_TUNNELING.req 168
STATUS 172
STATUS 174
RLC1 peer entities are tunneling not yet acknowledged data through RLC2 peer entities
178 CRLC_CONFIG.ind
CRLC_CONFIG.req 182
The network RLC1 entity is released.
CRLC_CONFIG.ind 176
CRLC_CONFIG.req 180
The UE RLC1 is released.

FIG. 6

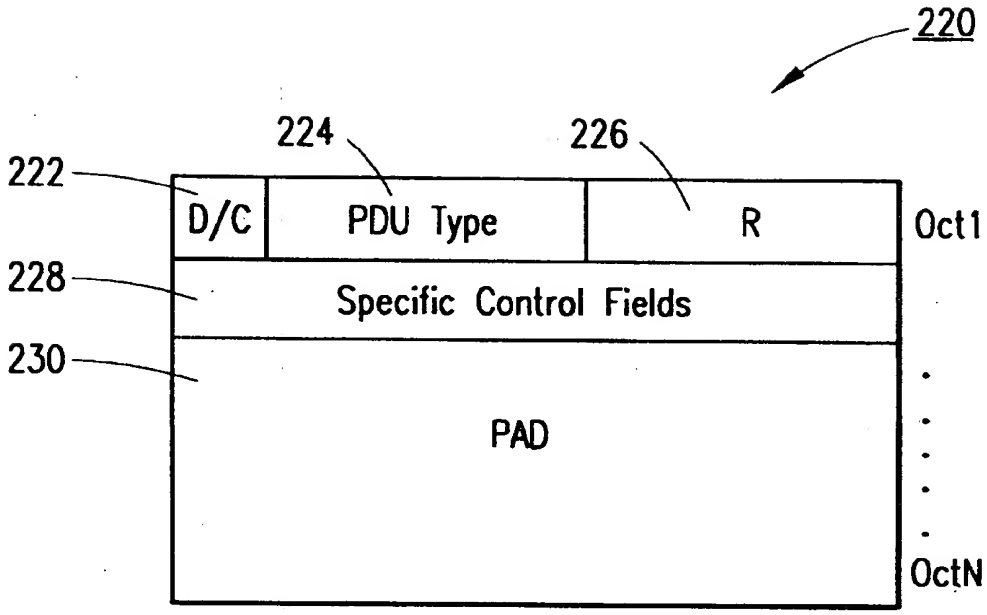

220
224
226
222
D/C
PDU Type
R
Oct1
228
Specific Control Fields
230
PAD
OctN

FIG. 8

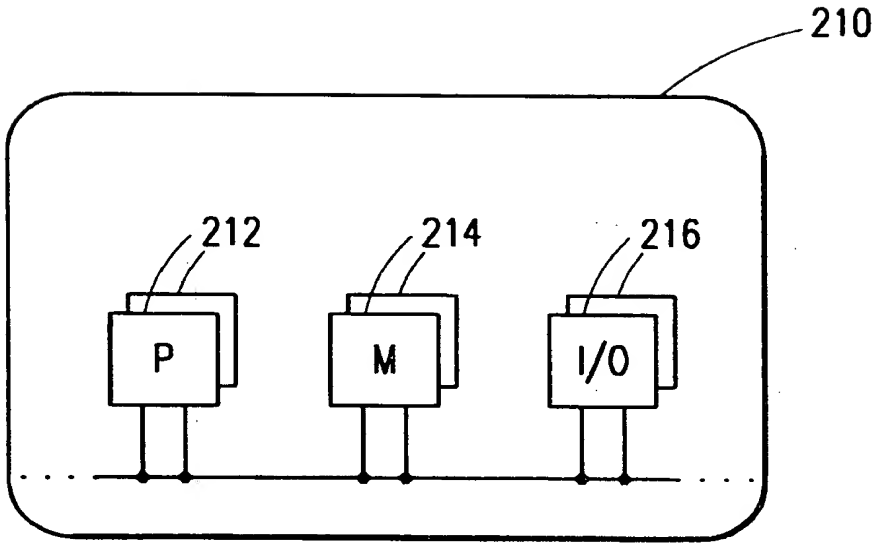


FIG. 9

TECHNIQUE FOR PROVIDING A SECURE LINK IN A MOBILE COMMUNICATION SYSTEM

FIELD OF THE INVENTION

The present invention relates generally to mobile communication systems and, more particularly, to a technique for providing a secure link when transitioning from a first pair of link layer protocol entities to a second pair of link layer protocol entities in a mobile communication system.

BACKGROUND OF THE INVENTION

Referring to FIG. **1**, there is shown a schematic diagram of a typical cellular mobile communication system **10**. The system **10** includes a Core Network (CN) **12**, a Radio Access Network (RAN) **14**, and a plurality of Mobile Stations (MS) **16**. The RAN **14** is divided into controller nodes **18** and Base Transceiver Station (BTS) nodes **20**. Of course, as will be appreciated by those having ordinary skill in the art, the RAN **14** may be made up of several RANs, each having one or more controller nodes **18** and BTS nodes **20**. The hierarchy of the system is such that the CN **12** is connected to several controller nodes **18**, each controller node **18** is connected to several BTS nodes **20**, and each BTS node **20** services one or more MS **16**.

Due to error characteristics associated with the radio interface between an MS **16** and a servicing BTS node **20**, an Automatic Repeat Request (ARQ) protocol can optionally be executed between the MS **16** and the RAN **14** to reduce the residual error rate. The function of the ARQ protocol is to take care of errors that are introduced as a result of the radio interface (e.g., due to interference). However, when the MS **16** moves around within the system **10**, a handover may occur that results in moving the execution of the ARQ protocol between different controller nodes **18**. To insure that no user data is lost during a handover, certain mechanisms must be implemented. There are presently three known mechanisms for securing user data in the case of a handover of the ARQ protocol between different controller nodes **18**.

In the first known mechanism for securing user data in the case of a handover of the ARQ protocol between different controller nodes **18**, which is adequately described by R. Cohen et al. in "Handover in a Micro-Cell Packet Switched Mobile Network", ACM Journal of Wireless Networks, Vol. 2, No. 1, 1996, pp. 13–25, and by E. Ayanoglu et al. in "AIRMAIL: A Link-Layer Protocol for Wireless Networks", ACM/Baltzer Wireless Networks Journal, Vol. 1, 1995, pp. 47–60, when the handover is performed, the entire protocol state, including the state variables and buffers, from the ARQ protocol entity in the RAN **14** are moved/transferred from an origination controller node **18** to a destination controller node **18**. Using this mechanism, the ARQ protocol entity in the MS **16** does not need to know when the handover occurs. In the case of a General Packet Radio Service (GPRS) system having two or more Serving GPRS Support Nodes (SGSN's) wherein an inter-SGSN handover takes place, only the downlink buffer is moved/transferred from the origination SGSN to the destination SGSN, and the protocol states of the buffers are synchronized between the MS **16** and the destination SGSN by means of handover signaling (see GSM 03.60—"Service Description").

The main benefits of this first mechanism are that no unnecessary re-transmission of the user data is required over the radio interface, and that the ARQ protocol in the MS **16** can be unaware of the handover, which also makes the implementation less expensive. However, this first mechanism is limited to intra-system handovers, where the same ARQ protocol with the same configuration is used throughout the system. Thus, it will no longer be useful in future systems where it will be possible to use different ARQ protocol configurations within the same RAN, and where there can be different sizes of protocol data units (PDU's) associated with the different ARQ protocol configurations. In addition, it can be very complex to move an entire protocol state.

In the second known mechanism for securing user data in the case of a handover of the ARQ protocol between different controller nodes **18**, which is specifically used in GPRS systems, the user data is secured by having 2 levels of ARQ protocols in the system **10**. The first ARQ protocol, called a Radio Link Control (RLC) protocol, is executed between an MS **16** and the RAN **14** (e.g., at a Base Station Controller (BSC) node) and is used to take care of errors that are introduced as a result of the radio interface (see GSM 04.60—"Radio Link Control/Medium Access Control"). The second ARQ protocol, called a Logical Link Control (LLC) protocol, is executed between an MS **16** and the CN **12** (e.g., at an SGSN node) (see GSM 04.64—"Logical Link Control (LLC) Layer Specification"). When a handover takes place, potentially lost user data is retransmitted by the ARQ protocol within the LLC protocol. The RLC protocol, on the other hand, is re-started in both the MS **16** and the BSC when a handover is performed.

The main benefit of this second mechanism is that it can handle inter-system handovers. However, this second mechanism has major disadvantages. For instance, unnecessary radio resources are wasted due to the overhead associated with the second ARQ protocol. In GPRS, the overhead that is transmitted with a third layer (L3) PDU is on the order of 7 bytes. This can be compared to the size of a Van Jacobsen compressed Transmission Control Protocol (TCP) acknowledgment, which is under 10 bytes when using a Point-to-Point Protocol (PPP). Thus, when transmitting TCP acknowledgments in an L3 PDU, the size is almost doubled. Another disadvantage of this second mechanism is that the cost in terms of memory and processing power of having 2 levels of ARQ protocols in the MS **16** is significantly higher than for a single ARQ protocol.

In the third known mechanism for securing user data in the case of a handover of the ARQ protocol between different controller nodes **18**, a sender of second layer (L2) ARQ protocol PDUs is required to keep all the L2 PDUs, carrying an L3 PDU, in a buffer until the whole L3 PDU has been acknowledged. Then, when a handover is performed, all the L3 PDUs are moved to the new L2_ARQ protocol entity, which then segments these L3 PDUs into new L2 PDUs and retransmits them.

Similar to the second mechanism, the main benefit of this third mechanism is that it can handle inter-system handovers. However, this third mechanism also has major disadvantages. For instance, extra buffer space is required because the sender of the L2_ARQ protocol PDUs is required to keep all the L2 PDUs, carrying a L3 PDU, in a buffer until the whole L3 PDU has been acknowledged. Also, when a handover takes place, all L2 PDUs of an L3 PDU are retransmitted by the new L2_ARQ protocol. That is, even the L2 PDUs which were previously acknowledged are retransmitted. This is of course not optimal and a major disadvantage of this third mechanism.

In view of the foregoing, it would be desirable to provide a technique for providing a secure link between a mobile

station and a core network during a handover or a protocol reconfiguration in a mobile communication system which overcomes the above-described inadequacies and shortcomings. More particularly, it would be desirable to provide a technique for providing a secure link between a mobile station and a core network during a handover or a protocol reconfiguration in a mobile communication system which does not transfer the entire state of an ARQ protocol, which does not use a second ARQ protocol level, which does not retransmit L2_ARQ PDUs which have already been acknowledged, and which does not need to store already acknowledged L2_ARQ PDUs in a buffer of the sending L2_ARQ protocol entity.

SUMMARY OF THE INVENTION

According to the present invention, a technique for providing a secure link when transitioning from a first pair of link layer protocol entities to a second pair of link layer protocol entities in a mobile communication system is provided. The first pair of link layer protocol entities includes a first transmitting link layer protocol entity for segmenting data and transmitting segmented data, and a first receiving link layer protocol entity for receiving segmented data from the first transmitting link layer protocol entity and acknowledging the received segmented data. The second pair of link layer protocol entities includes a second transmitting link layer protocol entity for segmenting data and transmitting segmented data, and a second receiving link layer protocol entity for receiving segmented data from the second transmitting link layer protocol entity and acknowledging the received segmented data. Both the first pair of link layer protocol entities and the second pair of link layer protocol entities are preferably automatic repeat request protocol entities.

The transition from the first pair of link layer protocol entities to the second pair of link layer protocol entities can be due to a variety of reasons such as, for example, a handover in the mobile communication system or a protocol reconfiguration in the mobile communication system. The first pair of link layer protocol entities can utilize the same protocol as the second pair of link layer protocol entities, or the first pair of link layer protocol entities can utilize a different protocol than the second pair of link layer protocol entities. If the first pair of link layer protocol entities utilizes the same protocol as the second pair of link layer protocol entities, the first pair of link layer protocol entities can still be configured differently than the second pair of link layer protocol entities.

In a preferred embodiment, the technique is realized by first suspending data transmissions from the first transmitting link layer protocol entity to the first receiving link layer protocol entity, and then initiating data transmissions from the second transmitting link layer protocol entity to the second receiving link layer protocol entity. The unacknowledged segmented data in the first transmitting link layer protocol entity is then tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

In accordance with other aspects of the present invention, the first pair of link layer protocol entities can be controlled by at least one first control protocol entity, and the second pair of link layer protocol entities can be controlled by at least one second control protocol entity. The data transmissions from the first transmitting link layer protocol entity to the first receiving link layer protocol entity can then be suspended by the at least one first control protocol entity, and the data transmissions from the second transmitting link layer protocol entity to the second receiving link layer protocol entity can then be initiated by the at least one second control protocol entity. It should be noted that the at least one first control protocol entity and the at least one second control protocol entity can be the same control protocol entity.

In accordance with further aspects of the present invention, untransmitted unsegmented data in the first transmitting link layer protocol entity is preferably transferred from the first transmitting link layer protocol entity to the second transmitting link layer protocol entity. Alternatively, untransmitted unsegmented data in the first transmitting link layer protocol entity can be segmented and then transferred from the first transmitting link layer protocol entity to the second transmitting link layer protocol entity for tunneling. Meanwhile, segmented data in the first transmitting link layer protocol entity can be assembled and transferred from the first transmitting link layer protocol entity to the second transmitting link layer protocol entity.

In accordance with still further aspects of the present invention, a status message can be sent from the first receiving link layer protocol entity to the first transmitting link layer protocol entity prior to tunneling the unacknowledged segmented data from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity. Also, the first receiving link layer protocol entity can be notified of the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity. If the first pair of link layer protocol entities are controlled by at least one first control protocol entity, and the second pair of link layer protocol entities are controlled by at least one second control protocol entity, then a sequence number of a last unacknowledged data segment in the first transmitting link layer protocol entity can be sent from the at least one first control protocol entity to the at least one second control protocol entity to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity. Alternatively, an indication of the number of tunneled unacknowledged segmented data can be sent from the at least one first control protocol entity to the at least one second control protocol entity to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity. Alternatively still, an indication of the amount of tunneled unacknowledged segmented data can be sent from the at least one first control protocol entity to the at least one second control protocol entity to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

In accordance with still further aspects of the present invention, a sequence number of a last unacknowledged data segment in the first transmitting link layer protocol entity can be sent from the first transmitting link layer protocol entity to the first receiving link layer protocol entity prior to tunneling the unacknowledged segmented data to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity. Alternatively, a message indicating that the previous tunneled unacknowledged segmented data was the last tunneled unacknowledged segmented data can be sent from the first transmitting link layer protocol entity to the first receiving link layer protocol entity after the last tunneled unacknowledged segmented data to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity. Alternatively still, a message containing an indication of the amount of tunneled unacknowledged segmented data can be sent from the second transmitting link layer protocol entity to the second receiving link layer protocol entity to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity. Alternatively even still, a message containing a sequence number of a last unacknowledged data segment in the first transmitting link layer protocol entity can be sent from the second transmitting link layer protocol entity to the second receiving link layer protocol entity prior to tunneling the unacknowledged segmented data to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity. If such is the case, the sequence number is signaled to the second transmitting link layer protocol entity from the first transmitting link layer protocol entity prior to sending the message, and then signaled to the first receiving link layer protocol entity from the second receiving link layer protocol entity after sending the message. Alternatively even still, an indication of the number of tunneled unacknowledged segmented data can be sent from the second transmitting link layer protocol entity to the second receiving link layer protocol entity to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity. If such is the case, the number of tunneled unacknowledged segmented data is signaled to the second transmitting link layer protocol entity from the first transmitting link layer protocol entity prior to sending the indication, and then signaled to the first receiving link layer protocol entity from the second receiving link layer protocol entity after sending the indication.

In accordance with still further aspects of the present invention, the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity can be signaled to the second transmitting link layer protocol entity from the first transmitting link layer protocol entity. A message indicating the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity can then be sent from the second transmitting link layer protocol entity to the second receiving link layer protocol entity. The end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity can then be signaled to the first receiving link layer protocol entity from the second receiving link layer protocol entity.

In accordance with still further aspects of the present invention, the first pair of link layer protocol entities can be terminated after all of the unacknowledged segmented data has been tunneled. Alternatively, the first pair of link layer protocol entities can be terminated after a predetermined period of time.

In accordance with still further aspects of the present invention, unacknowledged segmented data in the first transmitting link layer protocol entity can be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity by first sending the unacknowledged segmented data from the first transmitting link layer protocol entity to the second transmitting link layer protocol entity. The unacknowledged segmented data is then transmitted from the second transmitting link layer protocol entity to the second receiving link layer protocol entity. The unacknowledged segmented data is then sent from the second receiving link layer protocol entity to the first receiving link layer protocol entity.

In accordance with still further aspects of the present invention, the unacknowledged segmented data can be marked before it is transmitted from the second transmitting link layer protocol entity to the second receiving link layer protocol entity. The unacknowledged segmented data can be marked utilizing, for example, a length indicator field in an acknowledged mode data protocol data unit, or a special field in a control protocol data unit.

In accordance with still further aspects of the present invention, the unacknowledged segmented data can be transmitted from the second transmitting link layer protocol entity to the second receiving link layer protocol entity over a dedicated communication link. The unacknowledged segmented data is preferably transmitted from the second transmitting link layer protocol entity to the second receiving link layer protocol entity before any higher layer data so as to insure sequence order integrity.

In accordance with still further aspects of the present invention, tunneled unacknowledged segmented data is typically combined with acknowledged segmented data in the first receiving link layer protocol entity, and the combined segmented data is then assembled. The assembled combined data can then be sent directly to a higher layer protocol entity. Alternatively, the assembled combined data can be sent to a higher layer protocol entity through the second receiving link layer protocol entity. In any event, the

assembled combined data is preferably sent to a higher layer protocol entity before the second receiving link layer protocol entity sends any data to the higher layer protocol entity so as to insure sequence order integrity. Also, the second receiving link layer protocol entity can be notified that all the assembled combined data has been sent to the higher layer protocol entity so as to insure sequence order integrity.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to facilitate a fuller understanding of the present invention, reference is now made to the appended drawings. These drawings should not be construed as limiting the present invention, but are intended to be exemplary only.

FIG. **1** is a schematic diagram of a typical mobile cellular system including a Core Network (CN), a Radio Access Network (RAN), and a plurality of Mobile Stations (MS).

FIG. **2** is an illustration of a generic protocol stack for showing specific protocols on different hierarchical layers that are used within a cellular mobile communication system in accordance with the present invention.

FIG. **3** is a schematic diagram of a cellular mobile communication system including a CN, two different RANs, and an MS which are involved in a technique for providing a secure link between an MS and a CN during handover scenarios or L2_ARQ protocol reconfigurations in accordance with the present invention.

FIG. **4** is a flowchart showing data being transferred between two L2_ARQ protocol entities over an air interface.

FIG. **5** is a flowchart showing data being transferred between two new L2_ARQ protocol entities over an air interface just after a handover or an L2_ARQ protocol reconfiguration has taken place in accordance with the present invention.

FIG. **6** is a signaling chart for a handover scenario in accordance with the present invention.

FIG. **7** shows the format of an L2_ARQ Acknowledged Mode Data (AMD) PDU in accordance with the present invention.

FIG. **8** shows the format of an L2_ARQ Control PDU in accordance with the present invention.

FIG. **9** is a schematic diagram of an exemplary protocol entity processing device for implementing the signaling involved in a handover or a protocol reconfiguration in a mobile communication system in accordance with the present invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Referring to FIG. **2**, there is shown a generic protocol stack **50** which will be used in this detailed description to refer to specific protocols on different hierarchical layers that are used within a cellular mobile communication system operating in accordance with the present invention. It should be noted, however, that the present invention is not limited to the use of any one particular protocol on any of the different hierarchical layers. For instance, the L3 layer is used to refer to any network protocol such as, for example, Internet Protocol (IP). However, the L3 layer may also include a framing protocol such as, for example, Point-to-Point Protocol (PPP). The L3 layer may further include a control plane protocol such as, for example, Radio Resource Control (RRC), which is used in a Universal Mobile Telecommunication System (UMTS). Thus, the L3 layer refers to any protocol that produces a protocol data unit (PDU) that is transferred to the layer below, which in this case is the L2_ARQ layer.

The L2 ARQ layer is used to refer to a link layer protocol such as, for example, Radio Link Control (RLC), that potentially segments L3 PDUs into smaller L2_ARQ PDUs and/or concatenates several L3 PDUs into L2_ARQ PDUs and implements ARQ functionality on the basis of these L2_ARQ PDUs. Whatever protocol the L2_ARQ layer represents, the L2_ARQ protocol follows rules regarding the retransmission of L2 ARQ PDUs. For example, for any form of ARQ, the sending L2 ARQ has to buffer each L2_ARQ PDU until the receiving L2_ARQ positively acknowledges the receipt of same. Upon receiving the acknowledgment, the sending L2_ARQ is allowed to delete the acknowledged L2_ARQ PDU from its send buffer.

The L2_ARQ protocol may have several different operational modes such as, for example, unreliable, semi-reliable, and fully reliable, for the transmission of higher layer data (i.e., L3 PDUs). The latter two modes can either be combined with in-sequence or out-of-sequence delivery operation.

The L1 layer is used to refer to the physical layer of a radio link. It can be any radio transmission technology used in today's or future mobile communication networks (e.g., GSM, UMTS, or wireless LANs).

In state-of-the-art cellular mobile communication systems, there exist two peer entities of the L2_ARQ protocol, one running in a Mobile Station (MS) and one in a Radio Access Network (RAN). Examples of such systems are the Global System for Mobile Communications (GSM)/General Packet Radio Service (GPRS) and the UMTS systems, and the L2_ARQ protocol in both is the RLC protocol.

Referring to FIG. **3**, there is shown a cellular mobile communication system **100** which will be used in this detailed description to describe a technique for providing a secure link between an MS and a Core Network (CN) during handover scenarios or L2_ARQ protocol reconfigurations in accordance with the present invention. The system **100** comprises a CN **102**, which is connected to two different RANs **104**, and an MS **106**. As seen in FIG. **3**, L3 PDUs are transmitted between the MS **106** and the CN **102** through different L2_ARQ protocols depending on the currently used RAN **104**. The technique described in this detailed description is not limited to the number of RANs **104** that are connected to the CN **102**. That is, any number of RANs **104** are allowed by the technique described herein.

It is assumed that there exists peer-to-peer communication between any two L2_ARQ protocol entities for all of the different RANs **104** which are involved. The peer entities are executed in the MS **106** and in a network node of each RAN **104** which is involved. It is also assumed that handover can take place both within one RAN **104** (intra-system), and between different types of RANs **104** (inter-system). In either case, when a handover occurs, the execution point for the L2_ARQ protocol entity may be moved to a new physical network node where a new L2_ARQ protocol entity is started which continues the communication with a new L2_ARQ peer. Optionally, an old restarted/reinitialized L2_ARQ protocol entity may be used.

After a handover or an L2_ARQ protocol reconfiguration (e.g., a Radio Access Bearer (RAB) reconfiguration) has occurred, unacknowledged L2_ARQ PDUs in the old sending L2_ARQ protocol entity are tunneled through the new L2_ARQ protocol entities to the old receiving L2_ARQ

protocol entity. That is, after a handover or an L2_ARQ protocol reconfiguration has occurred, the old L2_ARQ protocol entities enter into a tunneling state wherein they do not perform any ARQ functions but still communicate data via the new L2_ARQ protocol entities. In this tunneling state, the old L2_ARQ PDUs are tunneled via the new L2_ARQ protocol entities to the old receiving L2_ARQ protocol entity, which reassembles the old L2_ARQ PDUs into L3 PDUs and delivers them to the receiving L3 protocol entity. After all the old L2_ARQ PDUs have been tunneled via the new L2_ARQ protocol entities to the old receiving L2_ARQ protocol entity, reassembled into L3 PDUs, and then delivered to the receiving L3 protocol entity, the old L2_ARQ protocol entities are terminated.

The above-described technique requires that a complete L3 PDU is either transmitted through the old sending L2_ARQ protocol entity or through the new sending L2_ARQ protocol entity. Thus, the last PDU in the old sending L2_ARQ protocol entity consists of a last segment of an old L3 PDU and possibly padding. On the receiving side, the new receiving L2_ARQ protocol entity receives new L2_ARQ PDUs from the new sending L2_ARQ protocol entity and reassembles them into L2_ARQ SDUs. The new L2_ARQ protocol entities have to distinguish between L2_ARQ SDUs containing new L3 PDUs and L2_ARQ SDUs containing tunneled old L2_ARQ PDUs. This can be achieved by marking the PDUs and/or the SDUs, or by other means of signaling. New L2_ARQ PDUs that contain tunneled old L2_ARQ PDUs are reassembled into old L2_ARQ PDUs and passed along to the old receiving L2_ARQ protocol entity. New L2_ARQ PDUs that contain new L3 PDUs are reassembled into L3 PDUs and delivered to the receiving L3 protocol entity.

The above-described technique can be better understood with reference to FIGS. **4** and **5**. FIG. **4** shows data being transferred between two L2_ARQ protocol entities over an air interface. Both the sending L2_ARQ protocol entity (i.e., L2_ARQ 1*a*) and the receiving L2_ARQ protocol entity (i.e., L2_ARQ 1*b*) comprise an SDU data buffer **110** and a PDU data buffer **112**. It shall be understood that these buffers are only logical buffers used for explaining the present invention. The data in the sending L2_ARQ protocol entity SDU data buffer **110***a* is higher layer data (i.e., L3 PDUs). This data has yet not been segmented into L2_ARQ PDUs or transmitted over the air interface by the sending L2_ARQ protocol entity (i.e., L2_ARQ 1*a*). The data in the sending L2_ARQ protocol entity PDU data buffer **112***a* consists of L2_ARQ PDUs. A PDU encapsulates either a part of an SDU or a full SDU. This is referred to as segmentation. If several SDUs are part of a PDU, then the several SDUs are referred to as being concatenated within the PDU.

It is assumed that an SDU resides in the sending L2_ARQ protocol entity SDU data buffer **110***a* until it is segmented and potentially concatenated and transferred to the sending L2_ARQ protocol entity PDU data buffer **112***a*. At that point, the whole SDU is moved into the sending L2_ARQ protocol entity PDU data buffer **112***a*. The PDUs sent from the sending L2_ARQ protocol entity (i.e., L2_ARQ 1*a*) over the air interface have to be acknowledged by the receiving L2_ARQ protocol entity (i.e., L2_ARQ 1*b*). When the sending L2_ARQ protocol entity receives an acknowledgement for a PDU, that PDU is discarded from the sending L2_ARQ protocol entity PDU data buffer **112***a*.

With the above definition of the buffers, it is understood that the sending L2_ARQ protocol entity PDU data buffer **112***a* may encapsulate both whole SDUs and parts of SDUs depending on what PDUs have been acknowledged by the sending L2_ARQ protocol entity. The data in the receiving L2_ARQ protocol entity PDU data buffer **112***b* will reside there until a whole SDU can be assembled. At that point, the assembled SDU will be transferred to the receiving L2_ARQ protocol entity SDU data buffer **110***b*.

FIG. **5** shows data being transferred between two new L2_ARQ protocol entities over an air interface just after a handover or an L2_ARQ protocol reconfiguration has taken place in accordance with the present invention. Both the old sending L2_ARQ protocol entity (i.e., L2_ARQ 1*a*) and the old receiving L2_ARQ protocol entity (i.e., L2_ARQ 1*b*) comprise an old SDU data buffer **114** and an old PDU data buffer **116**. Similarly, both the new sending L2_ARQ protocol entity (i.e., L2_ARQ 2*a*) and the new receiving L2_ARQ protocol entity (i.e., L2_ARQ 2*b*) comprise a new SDU data buffer **118** and a new PDU data buffer **120**. In this scenario, the old sending L2_ARQ protocol entity determines if PDUs in the old sending L2_ARQ protocol entity PDU data buffer **116***a* need to be reassembled into SDUs. If so, the reassembled SDUs are transferred to the old sending L2_ARQ protocol entity SDU data buffer **114***a*. The old sending L2_ARQ protocol entity SDU data buffer **114***a* will then contain SDUs encapsulating L3 PDUs, which are denoted as S1 in FIG. **5**. These SDUs (S1) in the old sending L2_ARQ protocol entity SDU data buffer **114***a* are then transferred along path **115** to the new sending L2_ARQ protocol entity SDU buffer **118***a*. Meanwhile, any PDUs remaining the old sending L2_ARQ protocol entity PDU data buffer **116***a*, which are denoted as P1 in FIG. **5**, are transferred along path **117** from the old sending L2_ARQ protocol entity PDU data buffer **116***a* to the new sending L2_ARQ protocol entity SDU data buffer **118***a*. These PDUs (P1) from the old sending L2_ARQ protocol entity PDU data buffer **116***a* serve as SDUs in the new sending L2_ARQ protocol entity. Additionally, new L3 PDUs are transferred directly between L3 and the new sending L2_ARQ protocol entity SDU data buffer **118***a* along path **119** after the handover/reconfiguration has occurred.

The data in the new sending L2_ARQ protocol entity SDU data buffer **118***a* is segmented and sent to the new sending L2_ARQ protocol entity PDU data buffer **120***a*. The data in the new sending L2_ARQ protocol entity PDU data buffer **120***a* is sent across the air interface to the new receiving L2_ARQ protocol entity PDU data buffer **120***b*. The data in the new receiving L2_ARQ protocol entity PDU data buffer **120***b* is assembled and sent to the new receiving L2_ARQ protocol entity SDU data buffer **118***b*. The data in the new receiving L2_ARQ protocol entity SDU data buffer **118***b* is either sent to the receiving L3 protocol entity or is sent to the old receiving L2_ARQ protocol entity PDU data buffer **116***b*. Any data in the old receiving L2_ARQ protocol entity PDU data buffer **116***b* is assembled and sent to the old receiving L2_ARQ protocol entity SDU data buffer **114***b* and then to the receiving L3 protocol entity.

Thus, in accordance with the present invention, any data (P1) which was residing in the old sending L2_ARQ protocol entity PDU data buffer **116***a* and transferred along path **117** from the old sending L2_ARQ protocol entity PDU data buffer **116***a* to the new sending L2_ARQ protocol entity SDU data buffer **118***a* at the time of the handover/reconfiguration is logically tunneled through tunnel **121** from the old sending L2_ARQ protocol entity PDU data buffer **116***a* to the old receiving L2_ARQ protocol entity PDU data buffer **116***b*.

There are mechanisms implemented in the new receiving L2_ARQ protocol entity which allow the new receiving L2_ARQ protocol entity to distinguish between L2_ARQ SDUs encapsulating tunneled old L2_ARQ PDUs and L2_ARQ SDUs encapsulating new L3 PDUs. These mechanisms are needed by the new receiving L2_ARQ protocol entity to correctly send the assembled L2_ARQ SDUs to the right buffer: the SDU data buffer **118***b* for new L3 PDUs and the PDU data buffer **116***b* for tunneled old L2_ARQ PDUs. This can be done by marking the PDUs and/or the SDUs, or, alternatively, by other rules combined with signaling.

If there is a rule that the data (P1) in the old sending L2_ARQ protocol entity PDU data buffer **116***a* is placed first in the new sending L2_ARQ protocol entity SDU data buffer **118***a*, then the new sending L2_ARQ protocol entity only needs to signal the number of L2_ARQ SDUs, or the number of new L2_ARQ PDUs, that encapsulate the tunneled old L2_ARQ PDUs in order for the receiver to distinguish between L3 PDUs and tunneled old L2_ARQ PDUs. The new receiving L2_ARQ protocol entity will then implicitly know where to send each assembled L2_ARQ SDU without having marked the PDUs and/or the SDUs. If concatenation of several L2_ARQ SDUs within a L2_ARQ PDU is supported by the new L2_ARQ protocol entities, together with signaling the number of new L2_ARQ PDUs including tunneled old L2_ARQ PDUs, then an additional rule will have to be defined. This rule defines that it is not possible to encapsulate a whole new L3 PDU in the last new L2_ARQ PDU including a tunneled old L2_ARQ PDU.

When marking is done there exist at least two different solutions. One solution is to allow two separate L2_ARQ PDU types, one corresponding to the new L3 PDUs and one corresponding to the PDUs that originate from the old sending L2_ARQ protocol entity (see description of FIG. 7 below). Another solution is to add a one bit field to the L2_ARQ SDU. This field can be set to one if the L2_ARQ SDU is actually a PDU from the old sending L2_ARQ protocol entity, and it can be cleared to zero if it is a new L3 PDU.

The old and the new sending L2_ARQ protocol entities must be able to communicate with each other, just as the old and the new receiving L2_ARQ protocol entities must be able to communicate with each other. These communication links are necessary to establish the tunneling state in accordance with the present invention. The communication links are logical links which can be divided into several physical links. For example, the L2_ARQ network protocol entities could be in different nodes of the radio access network and the logical link could be established via several physical links involving several network nodes of the radio access network and/or the core network. Alternatively, both protocol entities could reside in the same node and even in the same hardware/software (e.g., in the same processing device wherein the logical link could be one or several device components (see FIG. **9**)). In order to establish in-sequence delivery, the old receiving L2_ARQ protocol entity must signal to the new receiving L2_ARQ protocol entity that all of the old L2_ARQ PDUs are received correctly, reassembled into L3 PDUs, and delivered to the receiving L3 protocol entity. Only after that is the new receiving L2_ARQ protocol entity allowed to send SDUs to higher layers (i.e., the receiving L3 protocol entity).

When in the tunneling state, the old receiving L2_ARQ protocol entity needs to have knowledge about when the last old L2_ARQ PDU from the old sending L2_ARQ protocol entity has arrived. The present invention allows such information to be passed from the old sending L2_ARQ protocol entity to the old receiving L2_ARQ protocol entity.

One way to do this is by a rule stating that tunneled old L2_ARQ PDUs are placed first in the new receiving L2_ARQ protocol entity SDU data buffer **118***b* combined with signaling of the number of PDUs or SDUs holding tunneled old L2_ARQ PDUs. Then the new receiving L2_ARQ protocol entity implicitly knows when there are no more tunneled old L2_ARQ PDUs coming because it must be able to distinguish between L2_ARQ SDUs encapsulating new L3 PDUs and L2_ARQ SDUs encapsulating tunneled old L2_ARQ PDUs.

Another way to do this is to communicate the highest sequence number of the last old L2_ARQ PDU of the old sending L2_ARQ protocol entity to the old receiving L2_ARQ protocol entity. This sequence number may be transferred from the old sending L2_ARQ protocol entity to the old receiving L2_ARQ protocol entity via any appropriate signaling. Four solutions as to how this can be done are given below.

A first solution to this would be to signal the sequence number through a control protocol entity. This implies of course that the old L2_ARQ protocol entities inform the control protocol entity about this sequence number.

A second solution to this would be to send the sequence number in a special PDU (identified by a PDU Type field) containing the sequence number from the old sending L2_ARQ is protocol entity to the old receiving L2_ARQ protocol entity. This special PDU could be the first message to be transmitted before any L2_ARQ PDUs are tunneled. This special PDU is sent via the tunnel as well.

A third solution to this would be to send a special PDU (identified by a PDU Type field) after the last tunneled old L2_ARQ PDU from the old sending L2_ARQ protocol entity to the old receiving L2_ARQ protocol entity. This special PDU would indicate that the previous L2_ARQ PDU was the last L2_ARQ PDU to be tunneled. This special PDU is sent via the tunnel as well.

A fourth solution to this would be to send the sequence number in a special PDU (identified by a PDU Type field) containing the sequence number from the new sending L2_ARQ protocol entity to the new receiving L2_ARQ protocol entity. This special PDU would be the first message to be transmitted before any L2_ARQ PDUs are tunneled. The sequence number needs to be signaled from the old sending L2_ARQ protocol entity to the new sending L2_ARQ protocol entity and from the new receiving L2_ARQ protocol entity to the old receiving L2_ARQ protocol entity.

The knowledge about when the last tunneled L2_ARQ PDU has been received is used on the receiving side to know when the old receiving L2_ARQ protocol entity may be terminated. It is also necessary to enable in-sequence delivery of L3 PDUs at the receiver. The old receiving L2_ARQ protocol entity has to deliver all its data to the receiving L3 protocol entity and then indicate that it has finished before the new receiving L2_ARQ protocol entity may start delivering data to the receiving L3 protocol entity.

Referring to FIG. **6**, there is shown a signaling chart **130** for a handover scenario in accordance with the present invention. The particular example shown in FIG. **6** is based upon a UMTS system and involves a User Equipment Radio Resource Control protocol entity **132** (UE RRC), a first User Equipment Radio Link Control protocol entity **134** (UE RLC1), a second User Equipment Radio Link Control

protocol entity **136** (UE RLC2), a first Network Radio Link Control protocol entity **140** (NW RLC1), a second Network Radio Link Control protocol entity **138** (NW RLC2), a first Network Radio Resource Control protocol entity **142** (NW RRC1), and a second Network Radio Resource Control protocol entity **144** (NW RRC2). During a handover, the UE RRC entity **132** sends a cell update message **146** (CELL UPDATE) to the NW RRC1 entity **142**. In response, the NW RRC1 entity **142** requests the NW RRC2 entity **144** to set up a new RLC protocol entity using a configuration request message **148** (RRC_RLC_CONFIG.req). The NW RRC2 entity **144** then sets up the NW RLC2 entity **138** using a configuration request message **150** (CRLC_CONFIG.req). After the NW RLC2 entity **138** has been set up, the NW RRC2 entity **144** confirms the creation of the NW RLC2 entity **138** with the NW RRC1 entity **142** using a configuration confirmation message **152** (RRC_RLC_CONFIG.cfm). The NW RLC1 entity **140** is then suspended by the NW RRC1 entity **142** using a suspension request message **154** (CRLC_SUSPEND.req), which causes the NW RLC1 entity **140** to stop transmitting data and enter into the tunneling state described above. Next, the unsegmented SDUs in the NW RLC1 entity **140** are sent to the SDU buffer of the NW RLC2 entity **138** via an SDU transfer message **156** (SDU TRANSFER). A cell update confirmation message **158** (CELL UPDATE CONFIRM) is then sent from the NW RRC1 entity **142** to the UE RRC entity **132**. The cell update confirmation message **158** (CELL UPDATE CONFIRM) may contain an indication of the sequence number of the last PDU in the NW RLC1 entity **140**.

Upon receipt of the cell update confirmation message **158** (CELL UPDATE CONFIRM), the UE RRC entity **132** sets up the UE RLC2 entity **136** using a configuration request message **160** (CRLC_CONFIG.req). In addition, the UE RLC1 entity **134** is suspended by the UE RRC entity **132** using a suspension request message **162** (CRLC_SUSPEND.req), which causes the UE RLC1 entity **134** to stop transmitting data and enter into the tunneling state described above. Next, the unsegmented SDUs in the UE RLC1 entity **134** are sent to the SDU buffer of the UE RLC2 entity **136** via an SDU transfer message **164** (SDU TRANSFER). A cell update completion message **166** (CELL UPDATE COMPLETE) is then sent from the UE RRC entity **132** to the NW RRC1 entity **142**. The cell update completion message **166** (CELL UPDATE COMPLETE) may contain an indication of the sequence number of the last PDU in the UE RLC1 entity **134**.

At this point, there is no data transfer between the UE RLC1 entity **134** and the NW RLC1 entity **140**. That is, the UE is RLC2 entity **136** and the NW RLC2 entity **138** now perform the data transfer functions. However, any data remaining in the UE RLC1 entity **134** may now be tunneled through the UE RLC2 entity **136** once the UE RLC1 entity **134** receives a tunneling request message **168** (CRLC_TUNNELING.req) from the UE RRC entity **132**. Likewise, any data remaining in the NW RLC1 entity **140** may now be tunneled through NW RLC2 entity **138** once the NW RLC1 entity **140** receives a tunneling request message **170** (CRLC_TUNNELING.req) from the NW RRC1 entity **142**. It is desirable to start the tunneling with a status report, indicating which PDUs were received correctly, so that these need not be tunneled. For example, the UE RLC1 entity **134** sends a status report message **172** (STATUS) to the NW RLC1 entity **140**, while the NW RLC1 entity **140** sends a status report message **174** (STATUS) to the UE RLC1 entity **134**. The status report message **172** may also contain an indication of the sequence number of the last PDU in the UE RLC1 entity **134**. Similarly, the status report message **174** may also contain an indication of the sequence number of the last PDU in the NW RLC1 entity **140**.

After all the data in the UE RLC1 entity **134** has been tunneled and transmitted correctly, the UE RLC1 entity **134** indicates the same to the UE RRC entity **132** using a configuration indication message **176** (CRLC_CONFIG.ind). The UE RRC entity **132** then releases the UE RLC1 entity **134** using a configuration request message **180** (CRLC_CONFIG.req). Similarly, after all the data in the NW RLC1 entity **140** has been tunneled and transmitted correctly, the NW RLC1 entity **140** indicates the same to the NW RRC1 entity **142** using a configuration indication message **178** (CRLC_CONFIG.ind). The NW RRC1 entity **142** then releases the NW RLC1 entity **140** using a configuration request message **182** (CRLC_CONFIG.req).

At this point it should be noted that if in-sequence delivery is necessary, the UE RLC2 entity **136** and the NW RLC2 entity **138** should be notified that all UE RLC1 PDUs and all NW RLC1 PDUs have been received, respectively. After that, the UE RLC2 entity **136** and the NW RLC2 entity **138** can send the UE RLC2 SDUs and the NW RLC2 SDUs to higher layers, respectively.

At this point it should also be noted that the suspension request message **154** (CRLC_SUSPEND.req) and the suspension request message **162** (CRLC_SUSPEND.req) are somewhat misleading. In general, a protocol entity may be suspended, and then later may be resumed. In the particular example shown in FIG. **6**, however, the RLC1 entities **134** and **140** do not resume, but rather enter a tunneling state.

Referring to FIG. **7**, there is shown a format of an L2_ARQ Acknowledged Mode Data (AMD) PDU **190**, wherein L2_ARQ could be, for example, a Radio Link Control (RLC) protocol entity. The AMD PDU **190** includes a data/control (D/C) bit **192**, indicating if the PDU is an AMD PDU or a Control PDU, a sequence number (SN) field **194**, a poll (P) bit **196**, a header compression (H) bit **198**, one or more extension (E) bits **200**, zero or more length indicator fields **202**, one or more data segments **204**, and an optional field **206** containing padding (PAD) or a piggybacked status PDU (STATUS PDU). The extension bits **200** and the length indicator fields **202** can be of particular interest with respect to the present invention. The extension bit **200***a* indicates whether the next field will be data or a length indicator. The length indicator field **202** is used when concatenation or padding takes place in the PDU. In either case, it indicates where the concatenation or padding starts. If concatenation takes place, the length indicator field **202** indicates the border between the two higher layer segments. If padding takes place, the length indicator field **202** is assigned a specific value. The extension bit **200***b* is then set to indicate that the next octet will be yet another length indicator. The length indicator field **202** will then indicate the border between data and padding.

One of the length indicator fields **202** can also be used to indicate whether the data segments **204** contain tunneled RLC PDUs or L3 PDUs. To indicate the transport of tunneled RLC PDUs, the length indicator field **202** can be assigned a specific and reserved value.

Referring to FIG. **8**, there is shown a format of an L2_ARQ Control PDU **220**, wherein again L2_ARQ could be, for example, a Radio Link Control (RLC) protocol entity. The Control PDU **220** includes a data/control (D/C) bit **222**, indicating if the PDU is an AMD PDU or a Control PDU, a PDU Type field **224**, specifying the type of control message, a reserved field **226**, zero or more Specific Control Fields

228, depending on the type of control message, and padding (PAD) 230 to fill in the rest of the Control PDU 220. The Control PDU 220 can be used to transfer the sequence number of the, last untransmitted segmented L2_ARQ PDU of the old sending L2_ARQ protocol entity to the old receiving L2_ARQ protocol entity. The control message can be defined as either a PDU of the old L2_ARQ link, which is then tunneled via the new L2_ARQ link, or a PDU of the new L2_ARQ link, in which case a sequence number is signaled between the old and new L2_ARQ protocol entities. In order to define such a control message, a specific value for the PDU Type field 224 is defined and the Specific Control Field 228 contains the sequence number.

At this point it should be noted that the signaling associated with the above-described handover scenario is typically controlled by processors acting upon instructions stored in or transmitted to associated memory devices. For example, referring to FIG. 9, each of the above-described protocol entities may have an associated processing device 210 having at least one processor (P) 212, memory (M) 214, and input/output (I/O) device 216, connected to each other by a bus 218, for implementing the signaling involved in the above-described handover scenario.

The present invention is not to be limited in scope by the specific embodiments described herein. Indeed, various modifications of the present invention, in addition to those described herein, will be apparent to those of skill in the art from the foregoing description and accompanying drawings. Thus, such modifications are intended to fall within the scope of the appended claims.

What is claimed is:

1. A method for providing a secure link when transitioning from a first pair of link layer protocol entities to a second pair of link layer protocol entities in a mobile communication system, the first pair of link layer protocol entities including a first transmitting link layer protocol entity for segmenting data and transmitting segmented data and a first receiving link layer protocol entity for receiving segmented data from the first transmitting link layer protocol entity and acknowledging the received segmented data, the second pair of link layer protocol entities including a second transmitting link layer protocol entity for segmenting data and transmitting segmented data and a second receiving link layer protocol entity for receiving segmented data from the second transmitting link layer protocol entity and acknowledging the received segmented data, the method comprising the steps of:

suspending data transmissions from the first transmitting link layer protocol entity to the first receiving link layer protocol entity;

initiating data transmissions from the second transmitting link layer protocol entity to the second receiving link layer protocol entity; and

tunneling unacknowledged segmented data in the first transmitting link layer protocol entity from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

2. The method as defined in claim 1, further comprising the step of:

transferring untransmitted unsegmented data in the first transmitting link layer protocol entity from the first transmitting link layer protocol entity to the second transmitting link layer protocol entity.

3. The method as defined in claim 1, further comprising the step of:

segmenting untransmitted unsegmented data in the first transmitting link layer protocol entity;

transferring the untransmitted segmented data in the first transmitting link layer protocol entity from the first transmitting link layer protocol entity to the second transmitting link layer protocol entity for tunneling.

4. The method as defined in claim 1, further comprising the step of:

assembling segmented data in the first transmitting link layer protocol entity; and

transferring the assembled segmented data in the first transmitting link layer protocol entity from the first transmitting link layer protocol entity to the second transmitting link layer protocol entity.

5. The method as defined in claim 1, wherein the first pair of link layer protocol entities are controlled by at least one first control protocol entity, and the second pair of link layer protocol entities are controlled by at least one second control protocol entity, wherein the data transmissions from the first transmitting link layer protocol entity to the first receiving link layer protocol entity are suspended by the at least one first control protocol entity, and the data transmissions from the second transmitting link layer protocol entity to the second receiving link layer protocol entity are initiated by the at least one second control protocol entity.

6. The method as defined in claim 5, wherein the at least one first control protocol entity and the at least one second control protocol entity are the same control protocol entity.

7. The method as defined in claim 1, further comprising the step of:

sending a status message from the first receiving link layer protocol entity to the first transmitting link layer protocol entity prior to tunneling the unacknowledged segmented data from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

8. The method as defined in claim 1, further comprising the step of:

notifying the first receiving link layer protocol entity of the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

9. The method as defined in claim 8, wherein the first pair of link layer protocol entities are controlled by at least one first control protocol entity, and the second pair of link layer protocol entities are controlled by at least one second control protocol entity, further comprising the step of:

sending a sequence number of a last unacknowledged data segment in the first transmitting link layer protocol entity from the at least one first control protocol entity to the at least one second control protocol entity to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

10. The method as defined in claim 8, wherein the first pair of link layer protocol entities are controlled by at least one first control protocol entity, and the second pair of link

layer protocol entities are controlled by at least one second control protocol entity, further comprising the step of:

sending from the at least one first control protocol entity to the at least one second control protocol entity an indication of the number of tunneled unacknowledged segmented data to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

11. The method as defined in claim **8**, further comprising the step of:

sending a sequence number of a last unacknowledged data segment in the first transmitting link layer protocol entity from the first transmitting link layer protocol entity to the first receiving link layer protocol entity prior to tunneling the unacknowledged segmented data to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

12. The method as defined in claim **8**, further comprising the step of:

sending a message from the first transmitting link layer protocol entity to the first receiving link layer protocol entity after the last tunneled unacknowledged segmented data indicating that the previous tunneled unacknowledged segmented data was the last tunneled unacknowledged segmented data to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

13. The method as defined in claim **8**, further comprising the step of:

sending a message containing a sequence number of a last unacknowledged data segment in the first transmitting link layer protocol entity from the second transmitting link layer protocol entity to the second receiving link layer protocol entity prior to tunneling the unacknowledged segmented data to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

14. The method as defined in claim **13**, further comprising the steps of:

signaling the sequence number to the second transmitting link layer protocol entity from the first transmitting link layer protocol entity prior to sending the message; and

signaling the sequence number to the first receiving link layer protocol entity from the second receiving link layer protocol entity after sending the message.

15. The method as defined in claim **8**, further comprising the step of:

sending from the second transmitting link layer protocol entity to the second receiving link layer protocol entity an indication of the number of tunneled unacknowledged segmented data to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

16. The method as defined in claim **15**, further comprising the steps of:

signaling the number of tunneled unacknowledged segmented data to the second transmitting link layer protocol entity from the first transmitting link layer protocol entity prior to sending the indication; and

signaling the number of tunneled unacknowledged segmented data to the first receiving link layer protocol entity from the second receiving link layer protocol entity after sending the indication.

17. The method as defined in claim **8**, further comprising the step of:

sending a message from the second transmitting link layer protocol entity to the second receiving link layer protocol entity containing an indication of the amount of tunneled unacknowledged segmented data to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

18. The method as defined in claim **8**, wherein the first pair of link layer protocol entities are controlled by at least one first control protocol entity, and the second pair of link layer protocol entities are controlled by at least one second control protocol entity, further comprising the step of:

sending from the at least one first control protocol entity to the at least one second control protocol entity an indication of the amount of tunneled unacknowledged segmented data to notify the first receiving link layer protocol entity of the end of the unacknowledged segmented data tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

19. The method as defined in claim **8**, further comprising the steps of:

signaling to the second transmitting link layer protocol entity from the first transmitting link layer protocol entity the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity;

sending a message from the second transmitting link layer protocol entity to the second receiving link layer protocol entity indicating the end of the unacknowledged segmented data to be tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity; and

signaling to the first receiving link layer protocol entity from the second receiving link layer protocol entity the end of the unacknowledged segmented data to be

tunneled from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

20. The method as defined in claim **8**, further comprising the step of:

terminating the first pair of link layer protocol entities after all of the unacknowledged segmented data has been tunneled.

21. The method as defined in claim **1**, further comprising the step of:

terminating the first pair of link layer protocol entities after a predetermined period of time.

22. The method as defined in claim **1**, wherein the transition from the first pair of link layer protocol entities to the second pair of link layer protocol entities is due to a handover in the mobile communication system.

23. The method as defined in claim **1**, wherein the transition from the first pair of link layer protocol entities to the second pair of link layer protocol entities is due to a protocol reconfiguration in the mobile communication system.

24. The method as defined in claim **23**, wherein the first pair of link layer protocol entities utilize the same protocol as the second pair of link layer protocol entities.

25. The method as defined in claim **24**, wherein the first pair of link layer protocol entities is configured differently than the second pair of link layer protocol entities.

26. The method as defined in claim **23**, wherein the first pair of link layer protocol entities utilize a different protocol than the second pair of link layer protocol entities.

27. The method as defined in claim **1**, wherein the step of tunneling unacknowledged segmented data in the first transmitting link layer protocol entity from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity includes the steps of:

sending the unacknowledged segmented data from the first transmitting link layer protocol entity to the second transmitting link layer protocol entity;

transmitting the unacknowledged segmented data from the second transmitting link layer protocol entity to the second receiving link layer protocol entity; and

sending the unacknowledged segmented data from the second receiving link layer protocol entity to the first receiving link layer protocol entity.

28. The method as defined in claim **27**, further comprising the step of:

marking the unacknowledged segmented data before it is transmitted from the second transmitting link layer protocol entity to the second receiving link layer protocol entity.

29. The method as defined in claim **28**, wherein the unacknowledged segmented data is marked utilizing a length indicator field in an acknowledged mode data protocol data unit.

30. The method as defined in claim **28**, wherein the unacknowledged segmented data is marked utilizing a special field in a control protocol data unit.

31. The method as defined in claim **27**, wherein the unacknowledged segmented data is transmitted from the second transmitting link layer protocol entity to the second receiving link layer protocol entity over a dedicated communication link.

32. The method as defined in claim **27**, wherein the unacknowledged segmented data is transmitted from the second transmitting link layer protocol entity to the second receiving link layer protocol entity before any higher layer data so as to insure sequence order integrity.

33. The method as defined in claim **1**, further comprising the step of:

combining tunneled unacknowledged segmented data with acknowledged segmented data in the first receiving link layer protocol entity; and

assembling the combined segmented data.

34. The method as defined in claim **33**, further comprising the step of:

sending the assembled combined data directly to a higher layer protocol entity.

35. The method as defined in claim **33**, further comprising the step of:

sending the assembled combined data to a higher layer protocol entity through the second receiving link layer protocol entity.

36. The method as defined in claim **33**, further comprising the step of:

sending the assembled combined data to a higher layer protocol entity before the second receiving link layer protocol entity sends any data to the higher layer protocol entity so as to insure sequence order integrity.

37. The method as defined in claim **36**, further comprising the step of:

notifying the second receiving link layer protocol entity that all the assembled combined data has been sent to the higher layer protocol entity so as to insure sequence order integrity.

38. The method as defined in claim **1**, wherein the first pair of link layer protocol entities and the second pair of link layer protocol entities are automatic repeat request protocol entities.

39. An apparatus for providing a secure link when transitioning between pairs of link layer protocol entities in a mobile communication system, the apparatus comprising:

a first pair of link layer protocol entities, the first pair of link layer protocol entities including a first transmitting link layer protocol entity for segmenting data and transmitting segmented data and a first receiving link layer protocol entity for receiving segmented data from the first transmitting link layer protocol entity and acknowledging the received segmented data; and

a second pair of link layer protocol entities, the second pair of link layer protocol entities including a second transmitting link layer protocol entity for segmenting data and transmitting segmented data and a second receiving link layer protocol entity for receiving segmented data from the second transmitting link layer protocol entity and acknowledging the received segmented data;

wherein the first pair of link layer protocol entities are configured to suspend data transmissions from the first transmitting link layer protocol entity to the first receiving link layer protocol entity when transitioning from the first pair of link layer protocol entities to the second pair of link layer protocol entities;

wherein the second pair of link layer protocol entities are configured to initiate data transmissions from the second transmitting link layer protocol entity to the second receiving link layer protocol entity when transitioning from the first pair of link layer protocol entities to the second pair of link layer protocol entities; and

wherein the first pair of link layer protocol entities and the second pair of link layer protocol entities are configured to tunnel unacknowledged segmented data in the first transmitting link layer protocol entity from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity after transitioning from the first pair of link layer protocol entities to the second pair of link layer protocol entities.

40. An article of manufacture for providing a secure link when transitioning from a first pair of link layer protocol entities to a second pair of link layer protocol entities in a mobile communication system, the first pair of link layer protocol entities including a first transmitting link layer protocol entity for segmenting data and transmitting segmented data and a first receiving link layer protocol entity for receiving segmented data from the first transmitting link layer protocol entity and acknowledging the received segmented data, the second pair of link layer protocol entities including a second transmitting link layer protocol entity for segmenting data and transmitting segmented data and a second receiving link layer protocol entity for receiving segmented data from the second transmitting link layer protocol entity and acknowledging the received segmented data, the article of manufacture comprising:

at least one processor readable carrier; and

instructions carried on the at least one carrier; wherein the instructions are configured to be readable from the at least one carrier by at least one processor and thereby cause the at least one processor to operate so as to:

suspend data transmissions from the first transmitting link layer protocol entity to the first receiving link layer protocol entity;

initiate data transmissions from the second transmitting link layer protocol entity to the second receiving link layer protocol entity; and

tunnel unacknowledged segmented data in the first transmitting link layer protocol entity from the first transmitting link layer protocol entity to the first receiving link layer protocol entity through the second transmitting link layer protocol entity and the second receiving link layer protocol entity.

* * * * *

US006415151B1

(12) **United States Patent**
Kreppel

(10) **Patent No.: US 6,415,151 B1**
(45) **Date of Patent: Jul. 2, 2002**

(54) **METHOD AND MOBILE RADIO TELEPHONE NETWORK FOR HANDLING A PACKET DATA SERVICE**

(75) Inventor: **Jan Kreppel**, Penzberg (DE)

(73) Assignee: **Siemens Aktiengesellschaft**, Munich (DE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/347,211**

(22) Filed: **Jul. 2, 1999**

(30) **Foreign Application Priority Data**

Jul. 6, 1998 (DE) 198 30 164
Oct. 27, 1998 (DE) 198 49 578

(51) **Int. Cl.**[7] **H04Q 7/20**
(52) **U.S. Cl.** **455/445**; 455/417; 370/338; 370/401
(58) **Field of Search** 455/445, 417, 455/439, 446, 452, 450; 370/401, 338, 352, 353, 469, 409, 422; 379/207, 220, 221, 227, 229, 271, 273, 269

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,943,327	A *	8/1999	Mademann	370/329
5,970,059	A *	10/1999	Ahopelto et al.	370/338
5,978,386	A *	11/1999	Hamalainen et al.	370/466
5,996,021	A *	11/1999	Vivanlar et al.	709/238
6,101,539	A *	8/2000	Kennelly et al.	709/223
6,160,804	A *	12/2000	Ahmed et al.	370/349
6,233,458	B1 *	5/2001	Haumont et al.	455/445
6,256,300	B1 *	7/2001	Ahmed et al.	370/331
6,301,479	B1 *	10/2001	Roobol et al.	455/436
6,321,259	B1 *	11/2001	Ouellett et al.	709/220

FOREIGN PATENT DOCUMENTS

WO	WO 98/32304	*	7/1998	H04Q/7/38

OTHER PUBLICATIONS

GSM 03.78 version 5.5.0 Release 1996, TS 101 044, Digital cellular telecommunications system (Phase 2+); Customized Applications for Mobile network Enhanced Logic (CAMEL)—Stage 2, pp. 1–80.

GSM 03.60 version 6.1.1 Release 1997, Draft EN 301 344, Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2, pp. 1–102.

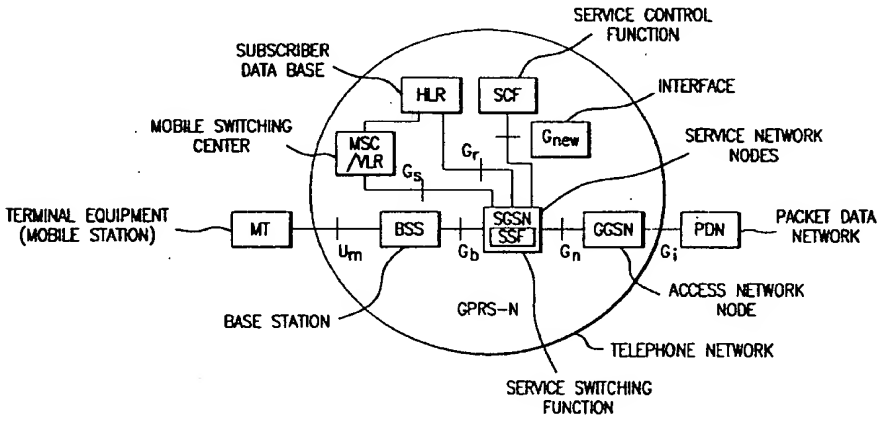
* cited by examiner

Primary Examiner—Nay Maung
Assistant Examiner—Sonny Trinh
(74) *Attorney, Agent, or Firm*—Morrison & Foerster LLP

(57) **ABSTRACT**

Proceeding from the handling of a packet data service in the mobile radio telephone network by at least one service network node (SGSNa, SGSNn) in conjunction with an access network node (GGSN) for the transmission of packet data, the following occurs. An interworking of the packet data service with network functions of an intelligent network whereof a service switching function (SSF) is interconnected with the respective service network node (SGSNa, SGSNn) and a service control function (SCF) is connected via an interface to the service network node (SGSNa, SGSNn) with integrated service switching function (SSF). Given change of the mobile subscriber from one coverage area into another coverage area, a switch is effected from an old association that exists between the service switching function (SSF) integrated in the previous service network node (SGSNa) and the service control function (SCF) to a new association that exists between the service switching function (SSF) integrated in the new service switching node (SGSNn) and the service control function (SCF). The switching is in addition to the switching from the one tunnel (TUa) to the other tunnel (TUb).

15 Claims, 6 Drawing Sheets



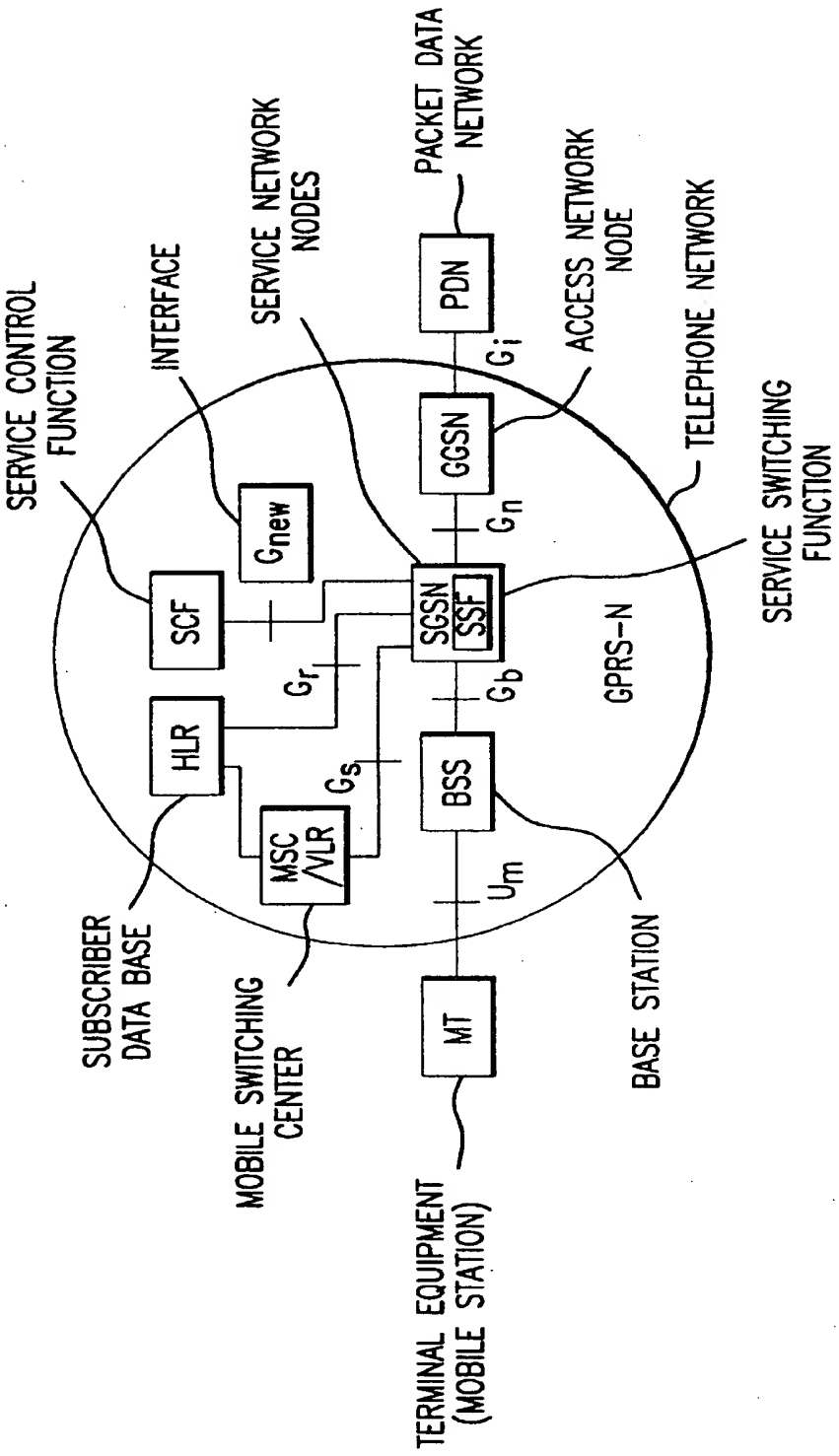

SERVICE CONTROL FUNCTION
INTERFACE
SERVICE NETWORK NODES
PACKET DATA NETWORK
ACCESS NETWORK NODE
TELEPHONE NETWORK
SERVICE SWITCHING FUNCTION
SCF
Gnew
PDN
GGSN
Gi
Gn
SGSN
SSF
Gr
Gb
GPRS-N
HLR
Gs
BSS
MSC /VLR
Um
SUBSCRIBER DATA BASE
MOBILE SWITCHING CENTER
BASE STATION
MT
TERMINAL EQUIPMENT (MOBILE STATION)

FIG. 1

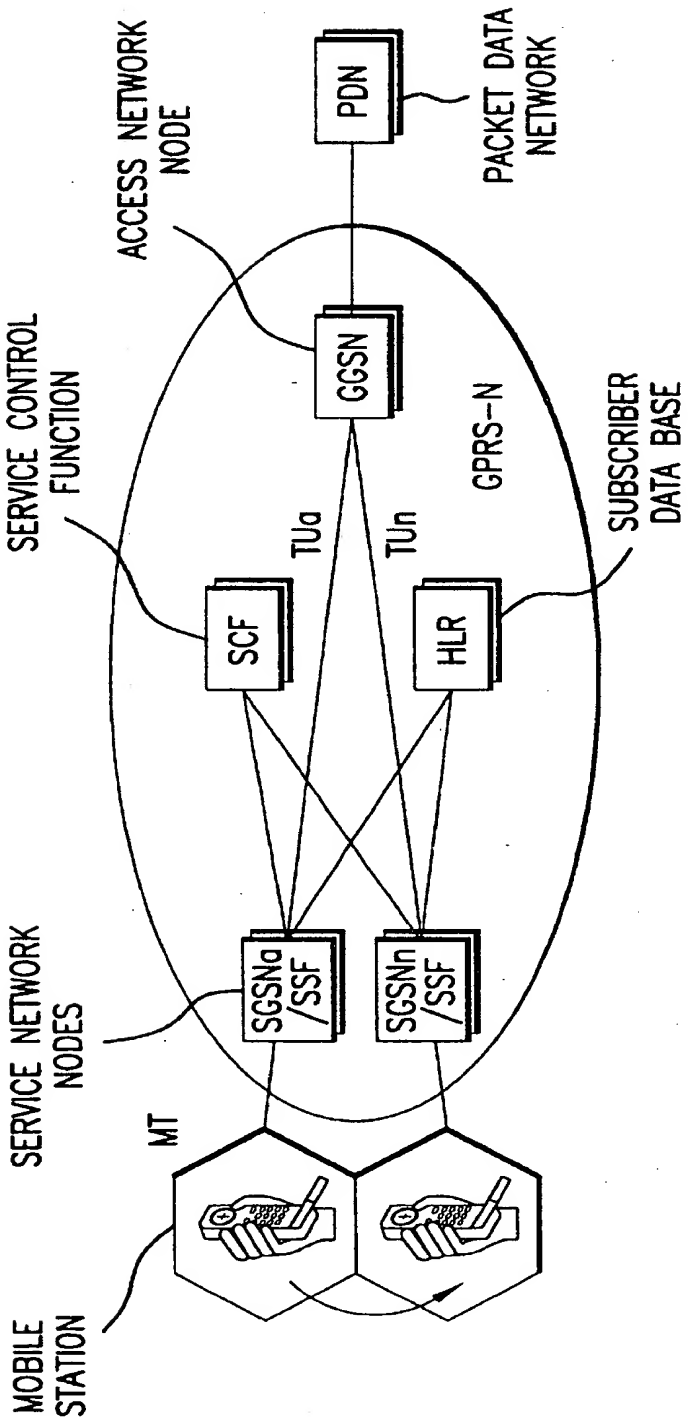

PDN
PACKET DATA NETWORK
ACCESS NETWORK NODE
GGSN
SERVICE CONTROL FUNCTION
GPRS-N
SUBSCRIBER DATA BASE
TUa
TUn
SCF
HLR
SGSNa /SSF
SGSNn /SSF
SERVICE NETWORK NODES
MT
MOBILE STATION

FIG. 2

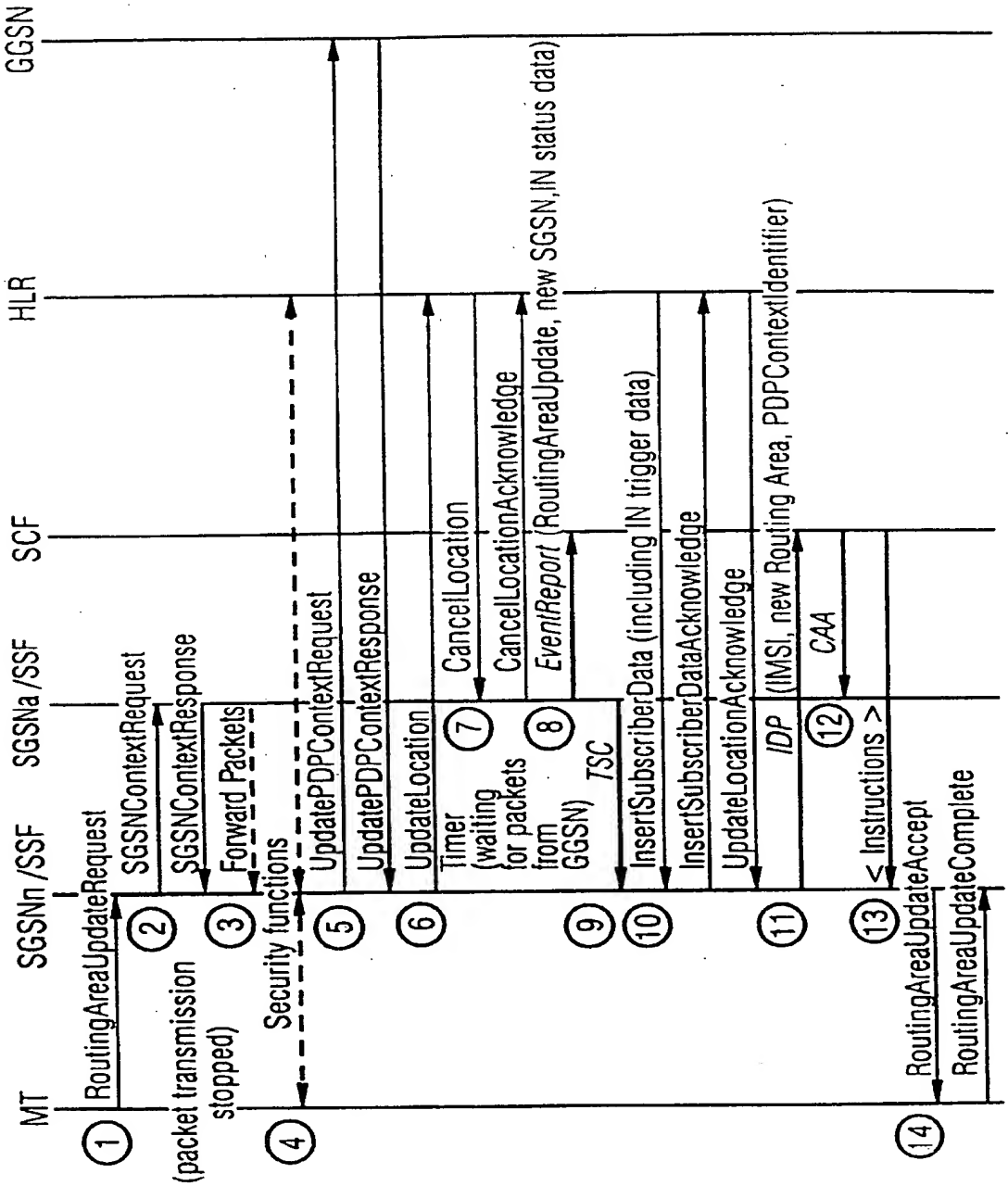

MT
SGSNn /SSF
SGSNa /SSF
SCF
HLR
GGSN
RoutingAreaUpdateRequest
SGSNContextRequest
SGSNContextResponse
Forward Packets
(packet transmission stopped)
Security functions
UpdatePDPContextRequest
UpdatePDPContextResponse
UpdateLocation
CancelLocation
Timer (waiting for packets from GGSN)
CancelLocationAcknowledge
EventReport (RoutingAreaUpdate, new SGSN,IN status data)
TSC
InsertSubscriberData (including IN trigger data)
InsertSubscriberDataAcknowledge
UpdateLocationAcknowledge
IDP (IMSI, new Routing Area, PDPContextIdentifier)
CAA
< Instructions >
RoutingAreaUpdateAccept
RoutingAreaUpdateComplete
1
2
3
4
5
6
7
8
9
10
11
12
13
14

FIG 3

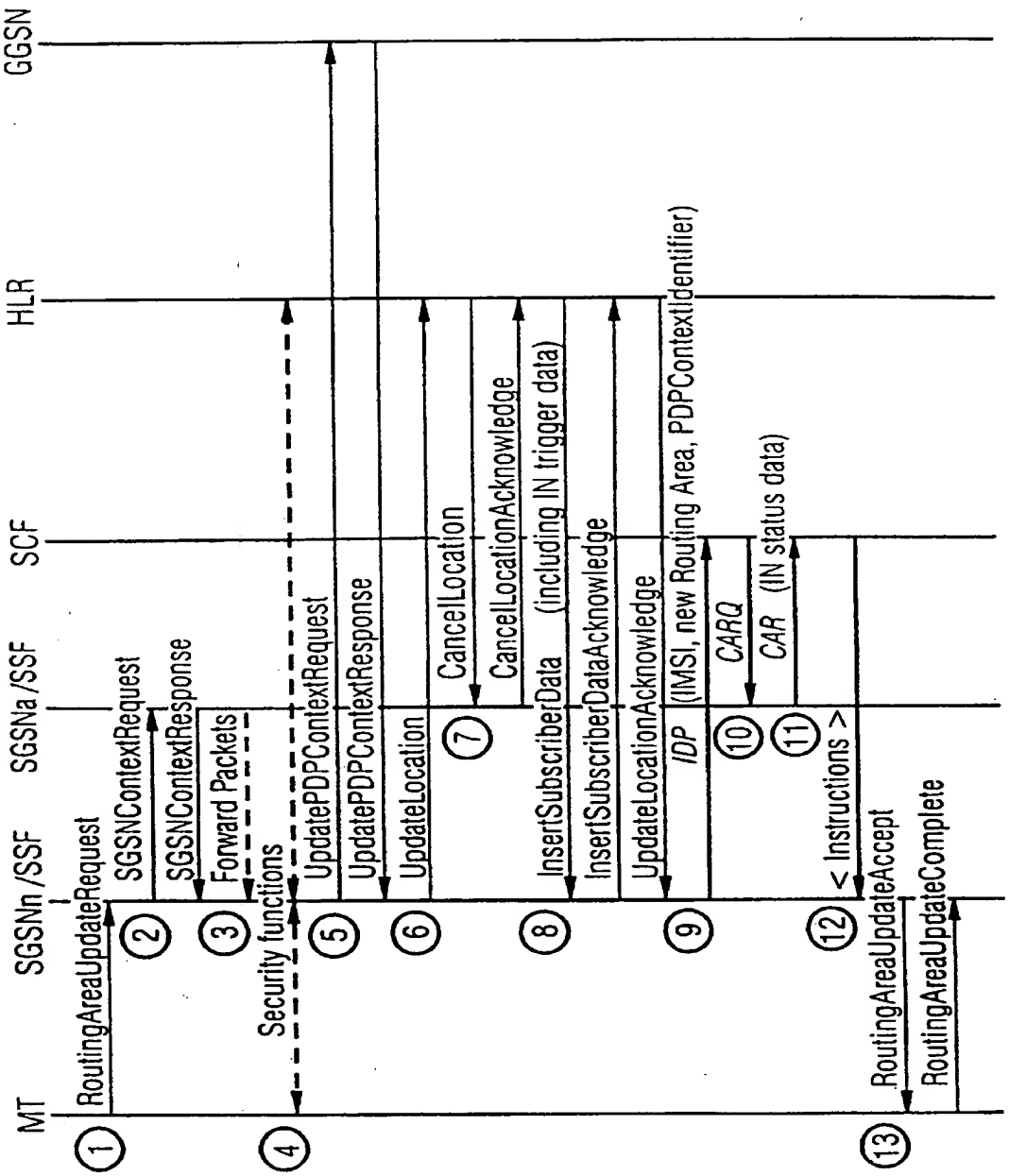

MT
SGSNn /SSF
SGSNa /SSF
SCF
HLR
GGSN
RoutingAreaUpdateRequest
SGSNContextRequest
SGSNContextResponse
Forward Packets
Security functions
UpdatePDPContextRequest
UpdatePDPContextResponse
UpdateLocation
CancelLocation
CancelLocationAcknowledge
InsertSubscriberData (including IN trigger data)
InsertSubscriberDataAcknowledge
UpdateLocationAcknowledge
IDP (IMSI, new Routing Area, PDPContextIdentifier)
CARQ
CAR (IN status data)
< Instructions >
RoutingAreaUpdateAccept
RoutingAreaUpdateComplete
1
2
3
4
5
6
7
8
9
10
11
12
13

FIG 4

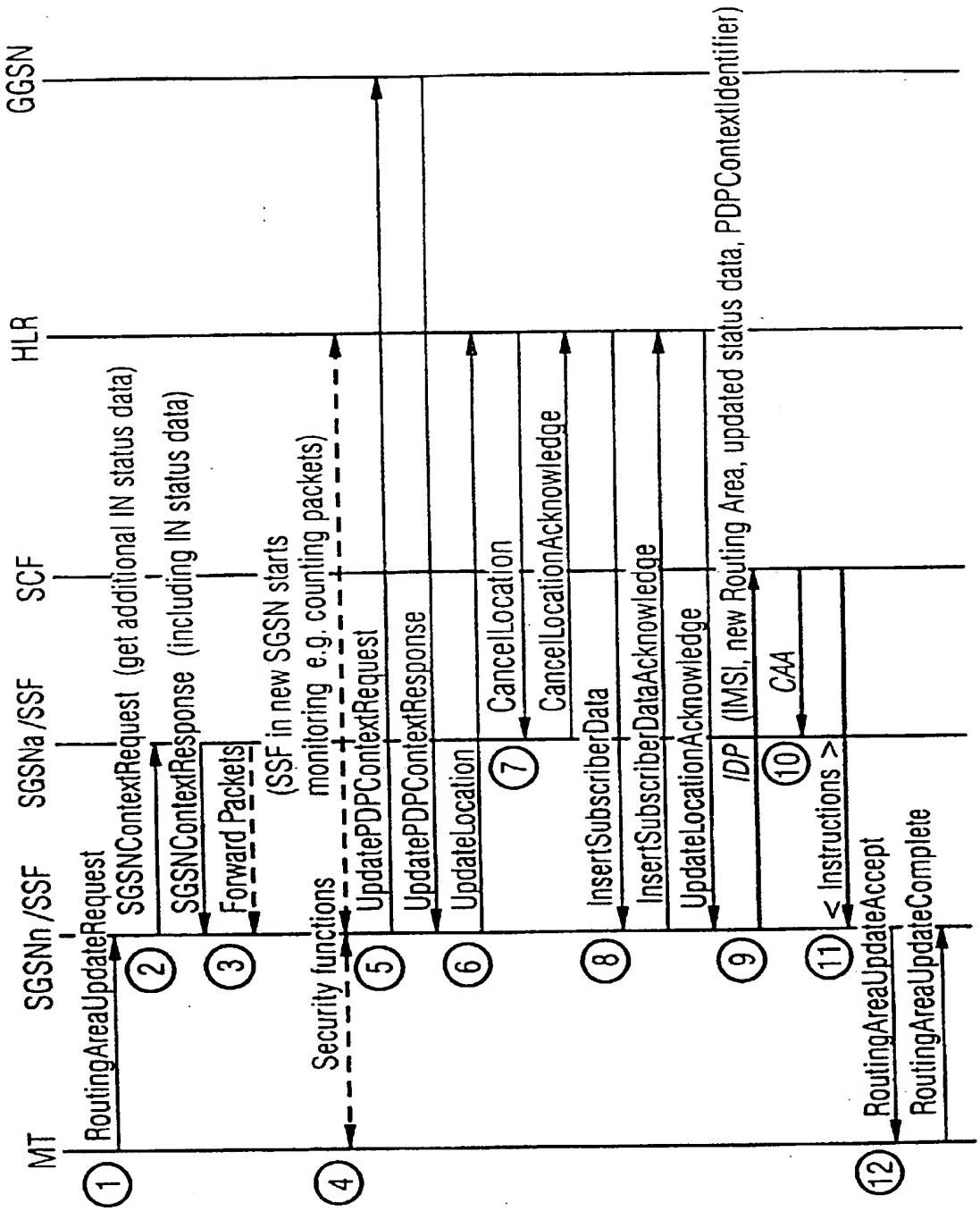

MT
SGSNn /SSF
SGSNa /SSF
SCF
HLR
GGSN
RoutingAreaUpdateRequest
SGSNContextRequest (get additional IN status data)
SGSNContextResponse (including IN status data)
Forward Packets
(SSF in new SGSN starts monitoring e.g. counting packets)
Security functions
UpdatePDPContextRequest
UpdatePDPContextResponse
UpdateLocation
CancelLocation
CancelLocationAcknowledge
InsertSubscriberData
InsertSubscriberDataAcknowledge
UpdateLocationAcknowledge
IDP (IMSI, new Routing Area, updated status data, PDPContextIdentifier)
CAA
< Instructions >
RoutingAreaUpdateAccept
RoutingAreaUpdateComplete
1
2
3
4
5
6
7
8
9
10
11
12

FIG 5

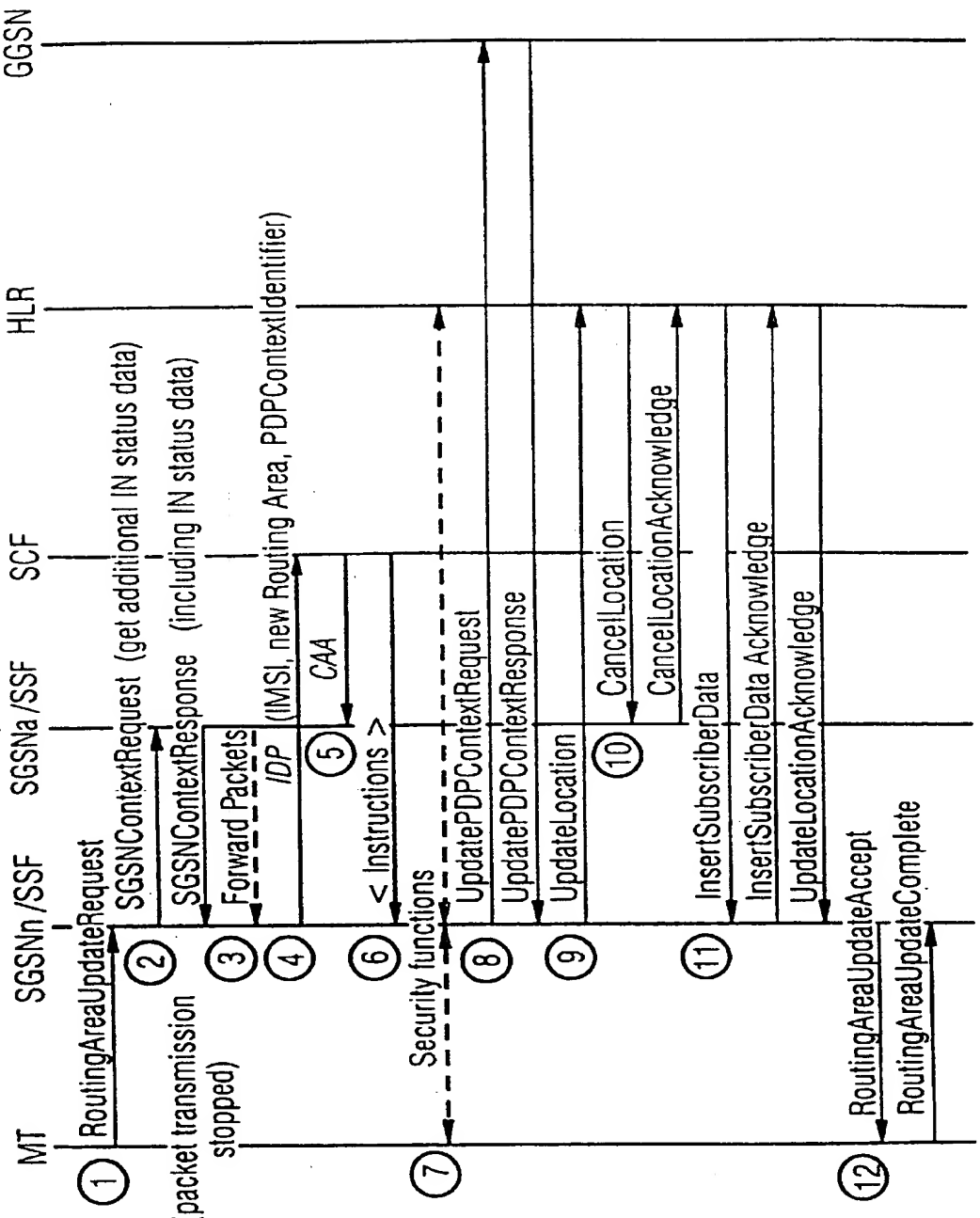

MT
SGSNn /SSF
SGSNa /SSF
SCF
HLR
GGSN
RoutingAreaUpdateRequest
SGSNContextRequest (get additional IN status data)
SGSNContextResponse (including IN status data)
Forward Packets
IDP
(IMSI, new Routing Area, PDPContextIdentifier)
CAA
< Instructions >
Security functions
UpdatePDPContextRequest
UpdatePDPContextResponse
UpdateLocation
CancelLocation
CancelLocationAcknowledge
InsertSubscriberData
InsertSubscriberData Acknowledge
UpdateLocationAcknowledge
RoutingAreaUpdateAccept
RoutingAreaUpdateComplete
(packet transmission stopped)
1
2
3
4
5
6
7
8
9
10
11
12

FIG 6

METHOD AND MOBILE RADIO TELEPHONE NETWORK FOR HANDLING A PACKET DATA SERVICE

BACKGROUND OF THE INVENTION

The present invention is directed to a method and to a mobile radio telephone network for handling a packet data service.

As known, it is possible to have the connections controlled by an intelligent network (IN) for connection-oriented communication services in a communication network. For example, a CAMEL platform (customized applications for mobile network enhanced logic) is thus defined according to the GSM Recommendation 03.78 for mobile radio telephone networks according to the GSM standard (global system for mobile communication) in order to enable a worldwide use of the performance features of the intelligent network. The standard architecture of the intelligent network provides a service switching function and a service control function that are connected to one another via a signaling link. A specific protocol that is composed of the CAP protocol (CAMEL application part) for the mobile radio telephone network is thereby employed as application.

New data services such as the packet data service GPRS (general packet radio service) according to GSM Recommendation 03.60 are being currently introduced in existing mobile radio telephone networks according to the GSM standard. The transmission in the mobile radio telephone network thereby does not occur connection-oriented but in the form of packet data. This type of transmission utilizes the given transmission resources in the mobile radio telephone network better. The architecture for the packet data service assumes that the communication terminal equipment used by the mobile subscriber—the mobile station—is services at its respective location by a service network node (serving GPRS support node). Access to a packet data network is necessary in order to receive or send packet data. To this end, access network nodes (gateway GPRS support nodes) are offered that respectively realize the access to the packet data network—for example, Internet—and support a specific packet data protocol—for example, Internet protocol. A tunnel via which the packets are transmitted is provided in the mobile radio telephone network between the service network node and the access network node. Since the mobile subscribers with their communication terminal equipment move between a plurality of radio coverage areas of a mobile radio telephone network, the individual subscriber may possibly proceed into the coverage area of a new service network node, so that the tunnel must be switched and the packets are to be transmitted on a new transmission path through the mobile radio telephone network. The previous service network node can no longer control the packet data service for the appertaining subscriber in this case.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a method and a mobile radio telephone network with which the use of the packet data surface can continue to be enabled for the mobile subscriber given a change of the coverage area.

Proceeding from the handling of a packet data service in the mobile radio telephone network by service network nodes in conjunction with an access network node for the transmission of packet data as well as a tunnel switching given a change of the coverage area, the following ensues. An interworking of the packet data service with network functions of an intelligent network whereof a service switching function is interconnected with the respective service network node and a service control function is connected via an interface to the service network node with integrated service switching function. Given the change of the mobile subscriber from the one coverage area into the other coverage area, a switching from an old association that exists between the service switching function integrated in the previous service network node and the service control function to a new association that exists between the service switching function integrated in the new service network node and the service control function ensues in addition to the switching from the one tunnel to the other tunnel. Only by combining integration of the service switching function into the respective service network node, communication with the service control function, and switching from old association to new association in addition to the switching of the tunnel for the packet data transmission, can packet data service be advantageously handled and controlled like other IN services and also continue to be available to the mobile subscriber (unnoticed and disturbance free) by application of IN functions given a change of the coverage area. The interface between the respective service network node with integrated service switching function and the service control function supports a uniform service handling even given a change of the coverage area, whereby the switching of the association is accompanied by the tunnel switching for the exchange of data, messages and signaling information.

According to a development of the invention, status data that are employed for switching the association between service switching function and service control function are reported from the previous service network node to the service control function before the end of the tunnel switching. The advantage of this modification lies therein that an association that already exists between the service switching function in the previous service network node and the service control function with respect to the subscriber who changes is utilized for reporting the association switching.

According to an alternative development of the invention, status data that are employed for switching the association between service switching function and service control function are requested by the service control function and are reported from the previous service network node. A direct communication between the service switching function the new service network node and the service control function results for information about the new responsibility for the packet data transmission.

According to another alternative development of the invention, status data that are employed for switching the association between service switching function and service control function are reported directly between the old service network node with integrated service switching function and the new service network node with integrated service switching function. In this version, a direct handover of the status data with respect to the association can already advantageously ensue during the interrogation of the new service network node, so that the new service network node is responsible from this moment on for monitoring the packet data stream and, due to the new association, can already supply the current data given log on at the service control function.

According to other beneficial versions of the invention, the new service network node with integrated service switching function reports at the service control function before or after the tunnel switching, continues the monitoring of the packet data transmission on the basis of the new association and makes the status data available to the service control function.

An advantageous development of the invention provides that the service control function receives data with reference whereto it recognizes that a switching of the association is involved and it can assume the monitoring of the packet data transmission.

BRIEF DESCRIPTION OF THE DRAWINGS

The features of the present invention which are believed to be novel, are set forth with particularity in the appended claims. The invention, together with further objects and advantages, may best be understood by reference to the following description taken in conjunction with the accompanying drawings, in the several Figures of which like reference numerals identify like elements, and in which:

FIG. 1 is a block circuit diagram of a mobile radio telephone network for handling the packet data service;

FIG. 2 is a block circuit diagram of the mobile radio telephone network when switching the tunnel for packet data transmission as well as the association given entry of the mobile subscriber into the coverage area of a new service network node;

FIG. 3 is a first version of the message flow between the network equipment of the mobile radio telephone network given change of the service network node;

FIG. 4 is a second version of the message flow between the network equipment given change of the service network node;

FIG. 5 is a further version of the message flow between the network equipment of the mobile radio telephone network given change of the service network node; and

FIG. 6 is a further version of the message flow between the network equipment of the mobile radio telephone network given change of the service network node.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The block circuit diagram of FIG. 1 shows the network architecture of a mobile radio telephone network GPRS-N for handling the packet data service GPRS. As known, the communication terminal equipment MT (the mobile station) of a mobile subscriber is wirelessly coupled to the mobile radio telephone network GPRS-N via an air interface Um, i.e. to the base station system BSS thereof with stationary base stations and base station controls. For the transmission of packet data between the mobile station MT and a packet data network PDN, the mobile radio telephone network GPRS-N comprises one or more service network nodes SGSN and at least one access network node GGSN. The access network node GGSN is thereby connected via an interface Gi to the packet data network PDN, whereas the service network node SGSN is connected to the base station system BSS via an interface Gb. For realizing switching-oriented functions in the mobile radio telephone network GPRS-N, a mobile switching center MSC with appertaining subscriber data base VLR is coupled to the service network node SGSN via an interface Gs and a subscriber data base HLR is connected to the service network node SGSN via an interface Gr. The registers VLR, HLR, as known, contain the subscriber data of the mobile subscriber, dependent on the location of his mobile station MT.

For handling the packet data service such as an IN service, an interworking of the packet data service ensues with network functions of an intelligent network (IN) whereof a service switching function SSF is interconnected with the service network node SGSN and a service control function SCF is connected via a new interface Gnew to the service network node SGSN with integrated service switching function SSF. Since the service network node SGSN has the necessary subscriber-related data available such as, for example, the current location, the identification data, etc., it is the optimum location for the IN linking. A packet relay that images the interface Gb to the base station system BSS onto the interface Gn to the access network node GGSN and that forwards the data packets in both directions is located in the service network node SGSN. This packet relay is used for the integration of the service switching function SSF in the service network node SGSN. The service switching function SSF is also additionally linked into the signaling at the Gb interface.

The following mechanisms are conceivable for initiating the IN services, including the packet data service:

Personally allocated IN services that are entered in the subscriber data base;

Permanently allocated IN services; and

IN services activated by the subscriber.

Initially, there is no connection in the network for the packet data service. In order to use the service, the mobile subscriber must first log on in the network (as in the case of connection-oriented services as well). On this occasion, the subscriber's identity and authorization are checked. In the second step, a packet data protocol must be activated. The network GPRS-N now establishes a tunnel between the respectively appertaining service network node SGSN and the access network node GGSN to the packet data network PDN. As a result, packets can be exchanged between the subscriber and the packet data network via this tunnel.

FIG. 2 shows the equipment of the mobile radio telephone network for handling the packet data service with intelligent network functions in case the mobile subscriber moves with his mobile station MT from the coverage area of a previous service network node SGSNa with integrated service switching function SSF to the coverage area of a new service network node SGSNn with integrated service switching function SSF. Differing from connection-oriented communication, a complete switching from an old tunnel TUa that proceeds between the previous service network node SGSNa with the integrated service switching function SSF and the access network node GGSN to a new tunnel TUn that proceeds between the new service network node SGSNn with the integrated service switching function SSF and the access network node GGSN now ensues in the mobile radio telephone network GPRS-N. The packet data now runs on the new path between the access network node GGSN and the new service network node SGSNn, i.e. the service switching function SSF in the old node SGSNa can no longer carry out its function for the appertaining subscriber. In addition to the tunnel switching, a switching between an old association that exists between the service switching function SSF integrated in the previous service network node SGSNa and the service control function SCF to a new association that exists between the service switching function SSF integrated in the new service network node SGSNn and the service control function SCF therefore occurs.

When changing the coverage area or, respectively, service network node SGSN, which results in the tunnel switching and, in particular, the association switching, a signaling occurs in the network GPRS-N between the new service network node SGSNn an the old service network node SGSNa as well as between the new service network node SGSNn and the access network node GGSN. Further, due to the respective association, messages are exchanged between

the old and the new service network node with integrated service switching function SSF and the service control function SCF or, respectively, the subscriber data base. The entire message traffic serves the purpose of switching the tunnel and the association and of maintaining the control and monitoring of the packet data transmission even given a change of the coverage area. Further, subscriber data are reported to the service network node SGSNn and the new location of the subscriber in the network is registered. There are a number of versions of the message flow according to FIG. 3 through FIG. 6 that sequences between the devices shown in FIG. 2 for this purpose.

FIG. 3 assumes that an association already exists between the old service network node SGSNa/SSF with integrated service switching function and the service control function SCF with respect to the subscriber who changes the coverage area or, respectively, the service network node. With respect to this association, the service control function SCF already previously sent instructions in order, for example, to implement a counting of the transmitted packets according to the packet data service. The following steps characterize the message flow:

(1): The mobile station MT sends a message Routing AreaUpdateRequest that proceeds to the new service network node SGSNn and with which an updating of the data in the network is requested on the basis of a change of the coverage area. The transmission of packets from the mobile station MT is temporarily suspended.

(2): The new service network node SGSNn sends the message SGSNContextRequest to the old service network node SGSNa in order to request the context data for the mobile station MT. The old service network node SGSNn sends the context data back in the message SGSNContext-Response.

(3): The old SGSN starts a timer and conducts packets that are still arriving via the previous tunnel (see FIG. 2) from the access network node GGSN to the new service network node SGSNn, where they are stored. The old service network node SGSNa must continue to count incoming packets and potentially monitor thresholds if this is necessary (see above under (1)). After the expiration of the timer, the context data for the subscriber are finally deleted and packets are no longer forwarded.

(4): The known security functions (including authentification) are implemented—according to the GGSN standard in the present example.

(5): With a message UpdatePDPContextRequest, the new service network node SGSNn now requests the access network node GGSN to switch from the old tunnel to the new tunnel (see FIG. 2). This acknowledges the request message with a message UpdatePDTPContextResponse.

(6): The new service network node SGSNn informs the home register HLR of the new location of the subscriber in a message UpdateLocation.

(7): With the message CancelLocation, the home register HLR requests that the old service network node SGSNa remove the subscriber from its data base. The deletion is confirmed with the message CancelLocationAcknowledge. The subscriber data, however, are only deleted after expiration of the timer if this is active. After expiration of the timer (or, respectively, if this is not active: after receipt of the message CancelLocation), the old service network node SGSNa can assume that the tunnel has been switched and new packets will no longer arrive from the access network node GGSN.

(8): The previous service network node SGSNa with integrated service switching function SSF now reports the change of subscriber to the service control function SCF in a message EvenReport. With this message, the service control function SCF is also informed that a switching to a new association is pending because of the change of coverage area, recognizable, for example, on the basis of data RoutingAreaUpdate, new SGSN that the message EventReport contains. Above all, status data INstatusdata are also sent in this EventReport message, these being employed for switching the association between the service switching function SSF and service control function SCF. A seamless transition to the new service network node SGSNn is thus implemented with an offering of the status data by the old service network node SGSNa before the end of the tunnel switching. Such status data can, for example, cover counter readings about transmitted and/or received packets, the address of the new service network node, charge data, etc. In the intelligent network, specific events lead to status changes and, thus, to a successive message exchange between the intelligent network function SSF and SCF. The triggering event ("event detection point") is the network-side reception of the message RoutingAreaUpdateRequest from the mobile station MT in the present example.

Based on the message EventReport, the service control function SCF recognizes that the subscriber has switched into the coverage area of the new service network node SGSNn, and switches into a status in which it waits for the new service network SGSNn to log on at it. Further actions can already be undertaken in the meantime, thus, for example, a charging of incurred fees on the basis of the reported counter readings.

(9): The old service network node SGSNa now sends a message TSC (TunnelSwitchingComplete) to the new service network node SGSNn in which it communicates that a switch has now been successfully made from the previous tunnel to the new tunnel and no further packets are present. This message advantageously serves for synchronization in order to prevent the new service network node SGSNn from logging on at the service control function SCF without having already obtained the log off from the old service network node SGSNa.

(10): The new service network node SGSNn receives the subscriber data from the home register HLR via the message InsertSubscriberData. The service network node SGSNn confirms this message with InsertSubscriberDataAcknowledge. The UpdateLocation procedure is terminated by the home register HLR UpdateLocation. Trigger data INtriggerdata are also located in the subscriber data, these signaling that the subscriber has subscribed to an IN service. It is likewise possible that it is permanently set within the new service network node SGSNn that the intelligent network must now be engaged.

(11): The new service network node SGSNn sends an initialization message IDP (InitialDetectionPoint) to the service control function SCF in which it communicates that the subscriber is now in its coverage area. This message IDP contains a plurality of data IMSI, newRoutingArea, PDNContextIdentifier, whereof the datum IMSI represents a subscriber identifier of the mobile subscriber, the datum newRoutingArea represents a coverage area identifier and the datum PDContextIdentifier represents an identifier of the respective packet data transmission. The datum PDContextIdentifier allows the service control function SCF to make an unambiguous identification of a packet "session" in the mobile radio telephone network. This is necessary when, for example, a plurality of packet data transmissions and, thus, a plurality of SCF/SSF associations exist for a subscriber. The datum PDContextIdentifier is already transmitted in the

message SGSNContextResponse to the new service network node SGSNn. The new service network node SGSNn/SSF with integrated service switching function now switches into a status in which it waits for instructions of the service control function SCF.

(12): On the basis of the message IDP of the new service network node SGSNn/SSF, the service control function SCF recognizes that it is a matter of the subscriber that was logged from the old service network node SGSNa. The service control function SCF now ends the association with the previous service network node SGSNa/SSF with integrated service switching function in final form. To that end, the message CAA (cancel association) is preferably sent to the service switching function SSF in the old service network node SGSNa, so that the latter receives the confirmation that the switch of the SSF/SCF association onto the new service network node SGSNn/SSF with integrated service switching function has ensued.

(13): The service control function SCF now sends new instructions in that, for example, new thresholds are defined for transmitted packets.

(14): The RoutingAreaUpdate procedure is terminated by the messages RoutingAreaUpdateAccept and RoutingAreaUpdateComplete. The packet transmission from/to the communication terminal equipment MT can be continued.

FIG. 4 shows another version of the message flow, whereby the change of the subscriber from the old service network node SGSNa as well as the status data are not actively reported to the service control function SCF; rather, the new service network node SGSNn logs on directly at the service control function SCF after the switching from the previous to the new tunnel. The service control function SCF subsequently ends the old association with the service switching function SSF integrated in the old service network node SGSNa and thereby requests terminating status data from it. The steps (1) through (6) of the message flow are identical to those of FIG. 3.

(7): The home register HLR requests the old service network node SGSNa to remove the subscriber from the data base (CancelLocation). This is confirmed with CancelLocationAcknowledge. The subscriber data, however, are not deleted until after the expiration of the timer, if this is active. After expiration of the timer (or, respectively, if this is not active: after receipt of the CancelLocation), the old service network node SGSNa can assume that the tunnel has been switched and new packets will no longer arrive from the access network node GGSN.

(8): The new service network node SGSNn receives the subscriber data from the home register HLR according to the message InsertSubscriberDataAcknowledge. The service network node SGSNn acknowledges this with the message InsertSubscriberDataAcknowledge. The UpdateLocation procedure is terminated by the home register HLR with the message UpdateLocationAcknowledge. The data Intriggerdata that indicate that the subscriber has subscribed to an IN service are also located in the subscriber data. It is likewise possible that it is permanently set within the service network node SGSNn that the intelligent network must now be engaged.

(9): The new service network node SGSN sends the initialization message IDP to the service control function SCF, informing it therein that the subscriber is now in its coverage area and, thus, is its responsibility. This message IDP contains the data IMSI, newRoutingArea, PDContextIdentifier that were already described with reference to FIG. 3. On the basis of the data in the message IDP, the new service network node SGSNn indicates the switching to a new SSF/SCF association. The new service network node SGSNn/SSF with integrated service switching function then switches into a status in which it waits for instructions from the service control function SCF.

(10): On the basis of the message IDP of the new service network node SGSNn/SSF, the service control function SCF recognizes that it is a matter of the subscriber that was logged off from the old service network node SGSNa. The service control function SCF now ends the previous association to the service switching function SSF integrated in the old service network node SGSNa by sending the message CARQ (CancelAssociationRequest) to the service network node SGSNa.

(11): The old service network node SGSNa answers with the message CAR (Cancel Association Response), whereby all status data of the previous association are co-transmitted (see (1)).

(12): Subsequently, the service control function SCF sends new instructions in that, for example, new thresholds for transmitted packets are defined.

(13): The RoutingAreaUpdate procedure is terminated by the messages RoutingAreaUpdateAccept and RoutingAreaUpdateComplete. The packet transmission from/to the communication terminal equipment MT can be continued.

In a further version according to FIG. 5, a direct handover of the status data with respect to the switching of the SSF/SCF association ensues between the old service network node SGSNa and the new service node SGSNn. The status data INstatusdata are already transmitted by the new service network node SGSNn during the context interrogation. Before the switch from the previous tunnel to the new tunnel, the new service network node SGSNn logs on at the service switching function SSF and continues the monitoring of the packet data transmission or, respectively, of the packet data stream on the basis of the new association. Upon log-on at the service control function SCF, the service switching function SSF in the new service network node SGSNn can thus already co-transmit the current status data early.

(1): The mobile station MT sends a RoutingAreaUpdateRequest message to the new service network node SGSNn. The transmission of packets from the mobile station MT is temporarily suspended. The new service network node SGSNn requests the context data from the old service network node SGSNa after receiving the RoutingAreaUpdate request.

(2): Status data INstatusdata that directly signal the new service network node SGSNn that a new SSF/SCF association exists for the subscriber are now incorporated into the response message SGSContextResponse of the old service network node SGSNa to the new service network node SGSNn. The status data INstatusdata (for example, counter readings for packets, etc.) are also contained in this message. From this point on, the packet data stream arriving from the access network node GGSN is no longer monitored by the service switching function SSF of the previous service network node SGSNa but by the new service network node SGSNn with integrated service switching function SSF. For the moment, however, a reporting of events to the service control function SCF is not yet possible.

(3): The old service network node SGSNa starts a timer and conducts packets that still arrive from the access network node GGSN via the tunnel to the new service network node SGSNn, where they are stored. The packets are counted in the new service network node SGSNn. After expiration of the timer, the subscriber context data are finally deleted and packets are no longer forwarded. The steps (4)

(authentication) through (12) (ending the Routing Update procedure) correspond to the steps in the procedure of FIG. 4. It is thereby advantageous that (according to Step (9)) the new association was already incorporated into the initialization message IDP and, thus, altered status data can be reported from the new service network node SGSNn to the service control function SCF.

In a further version according to FIG. 6, a direct handover of the status data with respect to the switching of the SSF/SCF association likewise ensues between the old service network node SGSNa and the new service network node SGSNn. The status data INstatusdata are already transmitted during the context interrogation by the new service network node SGSNn. Differing from FIG. 5, the log-on of the new service network node SGSNn at the service control function SCF only ensues after the switching from the previous tunnel to the new tunnel. The old service network node SGSNa retains the control of the packet data transmission before and during the switching. The Steps (1) through (3) are to be implemented according to the message flow according to FIG. 5. The necessary data for triggering the IN service (for example, CAMEL service indication) are thereby co-supplied from the old service network node SGSNa in the message SGSNContextResponse. Beginning immediately after the context interrogation, the service switching function SSF in the new service network node SGSNn already begins monitoring the packet data stream in order to be able to communicate status data to the service control function SCF later on demand.

The initialization message IDP with the data IMSI, newRoutingArea, PDContextIdentifier (described above) are already sent from the new service network node SGSNn to the service control function SCF in Step (4), it being communicated therein, among other things, that the subscriber is now in its coverage area and, thus, is under its responsibility.

In Step (5), the service control function SCF ends the previous association with the old service network node SGSNa/SSF with integrated service switching function by sending the message CAA (cancel association). According to Step (6), the new service network node SGSNn/SSF with integrated service switching function switches into a status in which it waits for instructions from the service control function SCF.

The remaining Steps (7) through (11) in FIG. 6 are identical to the Steps (4) through (8) according to FIG. 5. The Step (12) in FIG. 6 is the same as the Step (12) in FIG. 5, so that these Steps are implemented analogous to the above explanations and procedures.

The invention is not limited to the particular details of the method and apparatus depicted and other modifications and applications are contemplated. Certain other changes may be made in the above described method and apparatus without departing from the true spirit and scope of the invention herein involved. It is intended, therefore, that the subject matter in the above depiction shall be interpreted as illustrative and not in a limiting sense.

What is claimed is:

1. A method for handling a packet data service in a mobile radio telephone network, packet data being transmitted between a communication terminal equipment of a mobile subscriber and service network nodes of a mobile radio telephone network and an access network node of the mobile radio telephone network for the linking to a packet data network, and, given a change of A mobile subscriber from a coverage area of a previous service network node into a coverage area of a new service network node, a switch being made from a previous tunnel that proceeds between the previous service network node and the access network node to a new tunnel that proceeds between the new service network node and the access network node, comprising the steps of:

an interworking of the packet data service ensues with network functions of an intelligent network whereof a service switching function is interconnected with a respective service network node and a service control function is connected via an interface to the respective service network node with integrated service switching function; and

upon change of the mobile subscriber from one coverage area into another coverage area, a switch is carried out from an old association that exists between the service switching function integrated in the previous service network node and the service control function to a new association that exists between the service switching function integrated in the new service network node and the service control function, said switch being carried out in addition to the switching from the one tunnel to the other tunnel.

2. The method according to claim 1, wherein status data that is employed for switching the association between service switching function and service control function is reported from the previous service network node to the service control function before an end of the tunnel switching.

3. The method according to claim 2, wherein the status data is reported based on a message that is initiated by the service switching function integrated in the previous service network node.

4. The method according to claim 2, wherein the previous service network node sends a message to the new service node in which the previous service network node communicates that a successful switch has been made from the previous tunnel to the new tunnel and no further packets are present.

5. The method according to claim 1, wherein status data, that is employed for the switching of the association between service switching function and service control function is requested by the service control function and reported from the previous service network node.

6. The method according to claim 1, wherein status data, that is employed for switching the association between service switching function and service control function, is directly reported between the old service network node with integrated service switching function and the new service network node with integrated service switching function.

7. The method according to claim 6, wherein the new service network node with integrated service switching function logs on at the service control function before the tunnel switching and continues monitoring of the packet data transmission based on the new association and also makes the status data available to the service control function.

8. The method according to claim 6, wherein the new service network node with integrated service switching function logs on at the service control function after the tunnel switching and continues monitoring of the packet data transmission based on the new association and also makes status data available to the service control function.

9. The method according to claim 8, wherein the old service network node with integrated service switching function retains the monitoring of the packet data transmission before and during the tunnel switching.

10. The method according to claim 1, wherein data, is received by the service control function, based on the service

control function recognizing that a switching of the association is involved and the service control function can continue monitoring of the packet data transmission.

11. The method according to claim **10**, wherein the data contains at least one of the following: at least one subscriber identifier, an identifier of a respective packet data transmission, and a coverage area identifier.

12. The method according to claim **1**, wherein the new service network node with integrated service switching function sends an initialization message to the service control function which, in response thereto, sends a message for ending the previous association to the old service network node.

13. The method according to claim **12**, wherein the new service network node with integrated service switching function switches into a status in which the new service network node waits for instructions of the service control function with respect to further transmission of packet data.

14. The method according to claim **1**, wherein trigger data that signals the interworking with the network functions of the intelligent network are made available to the new service network node with integrated service switching function.

15. A mobile radio telephone network for handling a packet data service with an access network node for linking to a packet data network and with service network nodes for transmission of packet data from or to a communication terminal equipment of a mobile subscriber, the packet data transmission given a change of the mobile subscriber from a coverage area of a previous service network node into a coverage area of a new service network node is switchable from a previous tunnel that proceeds between the previous service network node and the access network node to a new tunnel that proceeds between the new service network node and the access network node, comprising:

for interworking of the packet data service with network functions of an intelligent network, a respective service network node being arranged such that the respective service network node is interconnected with a service switching function and such that a service control function is connected via an interface to the respective service network node with integrated service switching function; and

given a change of the mobile subscriber from the one coverage area into another coverage area, a switch being effectable from an old association that exists between the service switching function integrated in the previous service network node and the service control function to a new association that exists between the service switching function integrated in the new service network node and the service control function, being switchable in addition to the switching from the one tunnel to the other tunnel.

* * * * *

US006452915B1

(12) **United States Patent**
Jorgensen

(10) **Patent No.: US 6,452,915 B1**
(45) **Date of Patent: Sep. 17, 2002**

(54) **IP-FLOW CLASSIFICATION IN A WIRELESS POINT TO MULTI-POINT (PTMP) TRANSMISSION SYSTEM**

(75) Inventor: **Jacob W. Jorgensen**, Folsom, CA (US)

(73) Assignee: **Malibu Networks, Inc.**, El Dorado Hills, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/350,156**

(22) Filed: **Jul. 9, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/092,452, filed on Jul. 10, 1998.

(51) **Int. Cl.**[7] **H04Q 7/24**
(52) **U.S. Cl.** **370/338**; 370/328
(58) **Field of Search** 370/338, 328, 370/329, 230, 229, 231, 465, 466, 468, 232, 235; 455/455, 575, 525, 422, 426, 430, 437, 440, 11.1, 456, 404

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,742,512 A	5/1988	Akashi et al.	
4,907,224 A	3/1990	Scoles et al.	370/85.2
5,282,222 A	1/1994	Fattouche et al.	

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

CA	2064975	7/1999	
EP	702 462 A1	3/1996	H04B/7/08
EP	841 763 A1	5/1998	H04B/7/26
EP	848 563 A2	6/1998	H04Q/7/20

(List continued on next page.)

OTHER PUBLICATIONS

Bianchi, et al. "C–PRMA: A Centralized Packet Reservation Multiple Access for Local Wiresless Communications" in IEEE Transactions on Vehicular Technology, vol. 46, No. 2 pp. 422–436, May 1997.

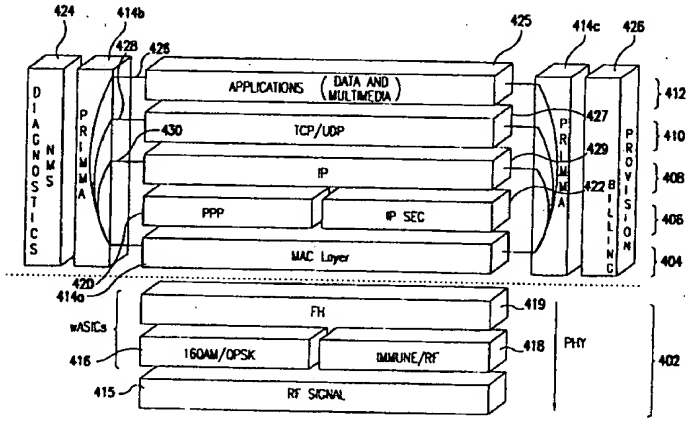
(List continued on next page.)

Primary Examiner—Douglas Olms
Assistant Examiner—Ricardo M. Pizarro
(74) *Attorney, Agent, or Firm*—Venable; Ralph P. Albrecht

(57) **ABSTRACT**

An IP flow classification system is used in a wireless telecommunications system. The IP flow classification system groups IP flows in a packet-centric wireless point to multi-point telecommunications system. The classification system includes: a wireless base station coupled to a first data network; one or more host workstations coupled to the first data network; one or more subscriber customer premise equipment (CPE) stations in wireless communication with the wireless base station over a shared bandwidth using a packet-centric protocol; and one or more subscriber workstations coupled to each of the subscriber CPE stations over a second network; a resource allocation device optimizes end-user quality of service (QoS) and allocates shared bandwidth among the subscriber CPE stations; an analyzing and scheduling device analyzes and schedules internet protocol (IP) flow over the shared wireless bandwidth. The analyzing device includes the above IP flow classifier that classifies the IP flow. The classifier can include a device for associating a packet of an existing IP flow with the IP flow. The classifier can include a QoS grouping device that groups a packet of a new IP flow into a QoS class grouping. The QoS grouping device can include a determining device that determines and takes into account QoS class groupings for the IP flow. The QoS grouping device can include an optional differentiated services (Diff Serv) device that takes into account an optional Diff Servs field priority marking for the IP flow.

163 Claims, 41 Drawing Sheets



U.S. PATENT DOCUMENTS

5,420,851	A		5/1995	Seshadri et al. 370/29
5,493,569	A		2/1996	Buchholz et al. 370/85.7
5,497,504	A		3/1996	Acampora et al.
5,499,243	A		3/1996	Hall
5,515,363	A		5/1996	Ben-Nun et al.
5,581,544	A		12/1996	Hamad et al.
5,602,836	A		2/1997	Papadopoulos et al. 370/280
5,613,198	A		3/1997	Ahmadi et al.
5,648,969	A		7/1997	Pasternak et al.
5,717,689	A		2/1998	Ayanoglu
5,724,513	A		3/1998	Ben-Nun et al.
5,729,542	A		3/1998	Dupont
5,732,077	A		3/1998	Whitehead
5,742,847	A		4/1998	Knoll et al.
5,752,193	A		5/1998	Scholefield et al.
5,757,708	A		5/1998	Eng et al.
5,787,077	A		7/1998	Kuehnel et al.
5,787,080	A		7/1998	Hulyalkar et al.
5,793,416	A		8/1998	Rostoker et al.
5,828,677	A		10/1998	Sayeed et al.
5,831,971	A		11/1998	Bonomi et al.
5,838,670	A		11/1998	Billström
5,841,777	A		11/1998	Cohen
5,864,540	A		1/1999	Bonomi et al.
5,907,822	A		5/1999	Prieto, Jr.
5,930,472	A	*	7/1999	Smith 713/200
5,936,949	A		8/1999	Pasternak et al.
5,956,330	A		9/1999	Kerns
5,970,059	A		10/1999	Ahopelto et al.
5,970,062	A		10/1999	Bauchot
5,974,028	A		10/1999	Ramakrishnan
5,974,085	A	*	10/1999	Smith 375/222
6,002,935	A		12/1999	Wang
6,005,868	A		12/1999	Ito
6,016,311	A		1/2000	Gilbert et al.
6,021,158	A		2/2000	Schurr et al.
6,031,832	A		2/2000	Turina
6,031,845	A		2/2000	Walding
6,038,230	A		3/2000	Ofek
6,038,452	A		3/2000	Strawczynski
6,041,051	A		3/2000	Doshi et al.
6,046,980	A	*	4/2000	Packer 370/230
6,052,594	A		4/2000	Chuang et al.
6,058,114	A		5/2000	Sethuram et al.
6,064,649	A		5/2000	Johnston
6,075,787	A		6/2000	Bobeck et al.
6,075,792	A		6/2000	Ozluturk
6,081,536	A		6/2000	Gorsuch et al.
6,084,867	A		7/2000	Meier
6,091,959	A	*	7/2000	Soussi 455/456
6,092,113	A		7/2000	Maeshima
6,097,722	A		8/2000	Graham et al.
6,097,733	A		8/2000	Basu et al.
6,104,721	A		8/2000	Hsu
6,111,863	A		8/2000	Rostoker et al.
6,115,357	A		9/2000	Packer et al.
6,115,370	A		9/2000	Struhsaker et al.
6,115,390	A		9/2000	Chuah
6,151,300	A		11/2000	Hunt et al.
6,151,628	A		11/2000	Xu et al.
6,154,643	A		11/2000	Cox
6,160,793	A		12/2000	Ghani et al.
6,163,532	A		12/2000	Taguchi et al.
6,195,565	B1		2/2001	Dempsey et al.
6,208,620	B1		3/2001	Sen et al.
6,215,769	B1		4/2001	Ghani et al.
6,219,713	B1		4/2001	Ruutu et al.
6,363,209	B2	*	7/2001	Reed 455/456
6,272,333	B1	*	8/2001	Smith 455/456
6,304,564	B1		10/2001	Monin et al.
6,320,846	B1		11/2001	Jamp et al.
6,330,451	B1		12/2001	Sen et al.

FOREIGN PATENT DOCUMENTS

EP	917 317 A1	5/1999	..... H04L/12/28
WO	WO 96/10320	4/1996	..... H04Q/7/22
WO	WO 98/37670	8/1998	..... H04L/12/56
WO	WO 99/26430	5/1999	..... H04Q/7/20
WO	WO 00722626	11/2000	
WO	WO 00/79722	12/2000	

OTHER PUBLICATIONS

Kim et al. "The AT&T Labs Broadband Fixed Wireless Field Experiment", IEEE Communications Magazine, Oct. 1999, pp. 56–62.

Iera et al. "Wireless Broadband Applications: The Teleservice Model and Adaptive QoS Provisioning", IEEE Communications Magazine, Oct. 1999, pp. 71–75.

Celidonio et al. "A Wedeband Two–Layer Radio Access Network Using DECT Technology in the Uplink", IEEE Communications Magazine, Oct. 1999, pp. 76–81.

Yoon et al. "A Wireless Local Loop System Based on Wideband CDMA Technology", IEEE Communications Magazine, Oct. 1999, pp. 128–135.

Balakrishman et al. "Improving Reliable Transprot and Handoff Performance in Cellular Wireless Networks", http://www.cs.berkely.edu/~ss/papers/wunet/html/winet.hml., Computer Science Div., Dept. of Electrical Engineering and Computer Science, Univ. of California at Berkeley, Berkeley, CA 94720–1776, Nov. 1995, pp. 1–18.

"A Cellular Wireless Local Area Network with QoS Guarantees for Heterogeneous Traffic", Authur(s): Sunghyun Choi and Kang G. Shin, *Technical Report CSE–TR–300–96*, Aug. 1996, pp. 1–24.

"The GSM System", Authors: Michel Mouly, Marie–Bernadette Pautet, pp. 272–277, XP–002154762.

"A Comparison of Mechanisms for Improving TCP Performance over Wireless Links" Author(s): Hari Balakrishnan, Venkata N. Padmanabhan, Srinvasan Seshan, and Randy H. Katz; XF000734405 *IEEE/ACM Transactions on Networking*, vol. 5, No. 6, Dec. 1997, pp. 756–769.

"Improving TCP/IP Performance Over Wireless Networks"; Author(s): Hari Balakrishnan, Srinivasan Seshan, Elan Amire and Randy H. Katz; *In Proc. 1st ACM Int'l Conf. On Mobile Computing and Networking (Mobicom)*, Nov. 1995, XP–002920962.

International Search Report; Date: Dec. 14, 2000; International Appln. No. PCT/US 00/18531 for (36792–164878).

International Search Report; Date: Feb. 14, 2000; International Appln. No. PCT/US 00/18584 for (36792–164879).

International Search Report; Date: Dec. 14, 2000; International Appln. No. PCT/US 00/18585 for (36792–164880).

International Search Report; Date: Dec. 22, 2000; International Appln. No. PCT/US 00/18666 for (36792–164881).

* cited by examiner

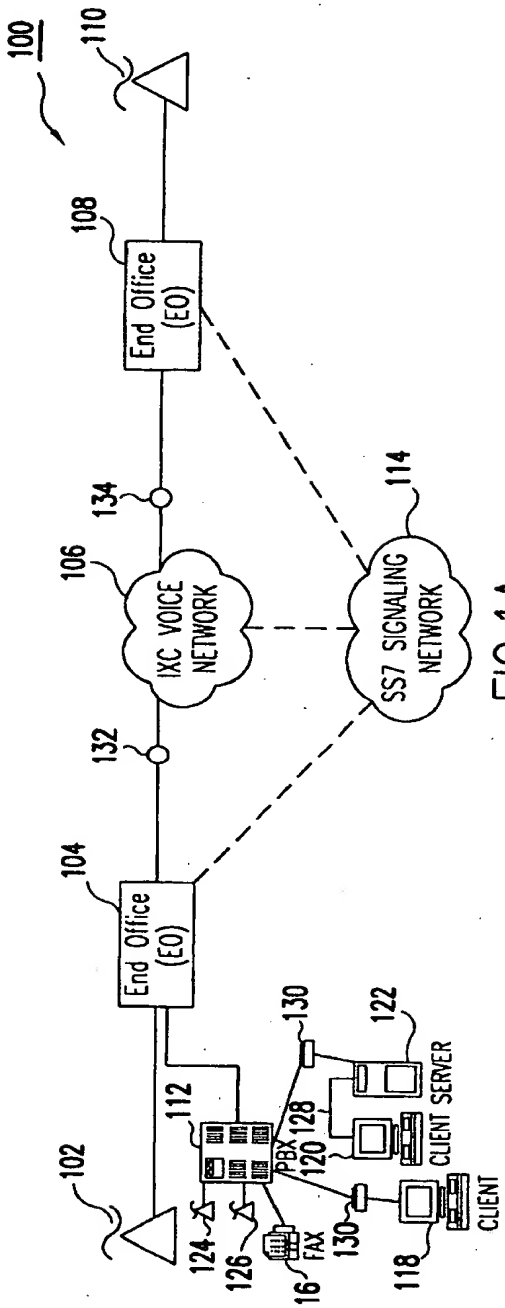


FIG. 1A

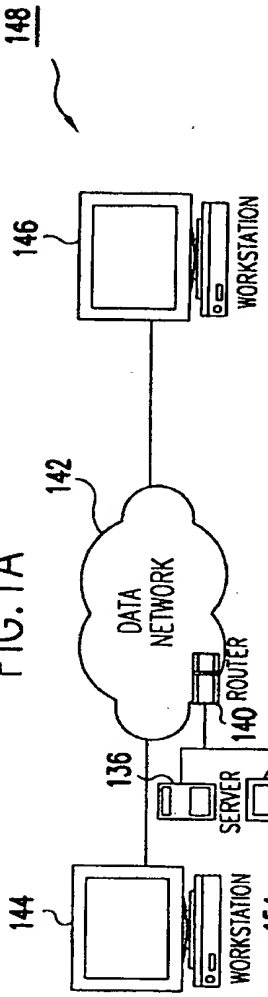


FIG. 1B

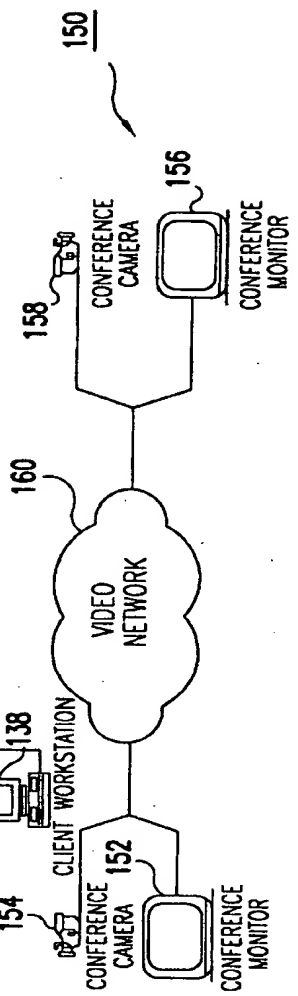


FIG. 1C

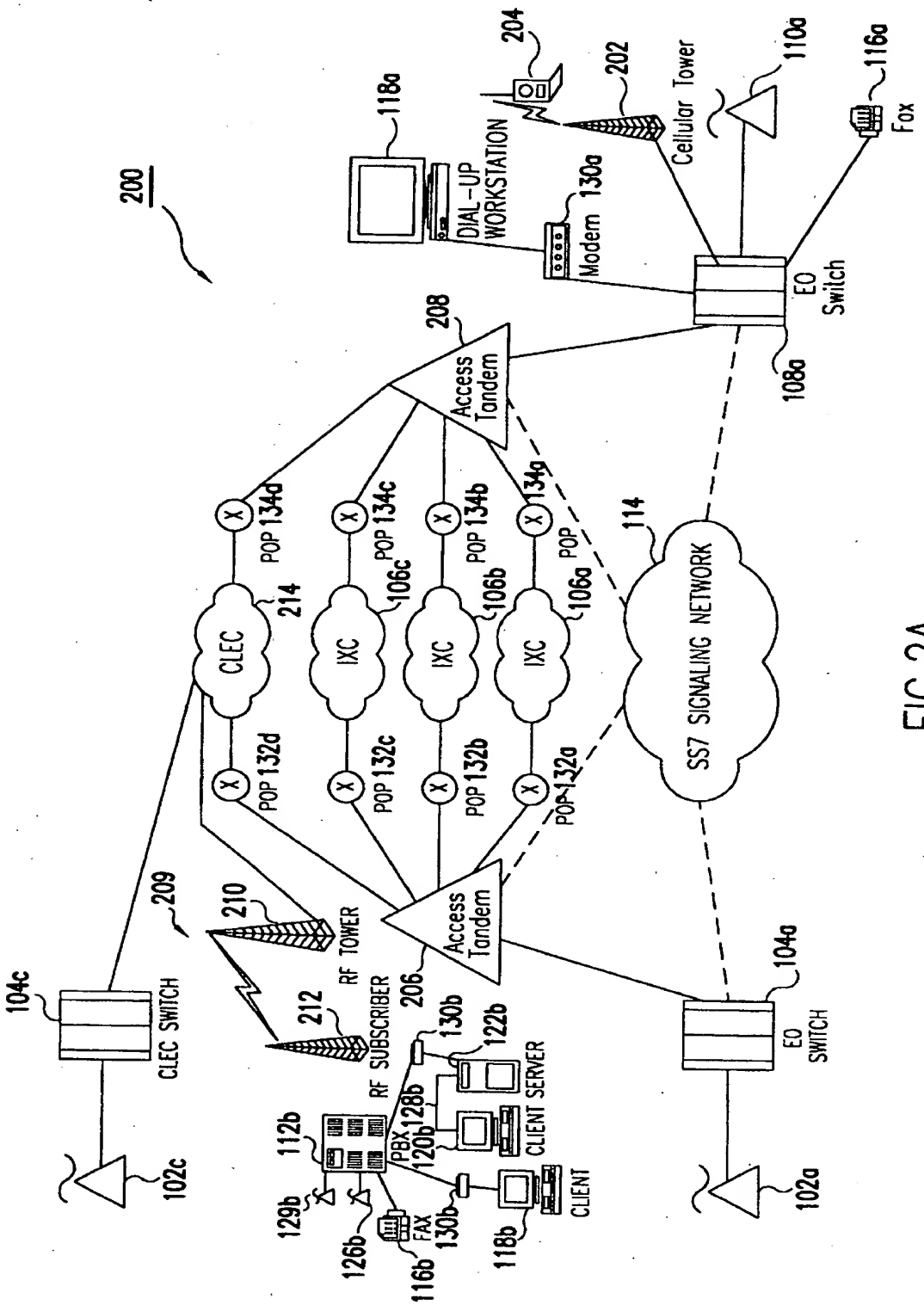

200
118a
DIAL-UP WORKSTATION
204
202
Cellular Tower
110a
116a
Fax
Modem 130a
EO Switch
108a
208
Access Tandem
114
SS7 SIGNALING NETWORK
POP 134d
POP 134c
POP 134b
POP 134a
214
CLEC
IXC
IXC
IXC
106c
106b
106a
POP 132d
POP 132c
POP 132b
POP 132a
209
210
RF TOWER
212
RF SUBSCRIBER
206
Access Tandem
104c
CLEC SWITCH
104a
EO SWITCH
130b
122b
CLIENT SERVER
128b
120b
112b
PBX
129b
126b
FAX
116b
130b
118b
CLIENT
102c
102a

FIG.2A

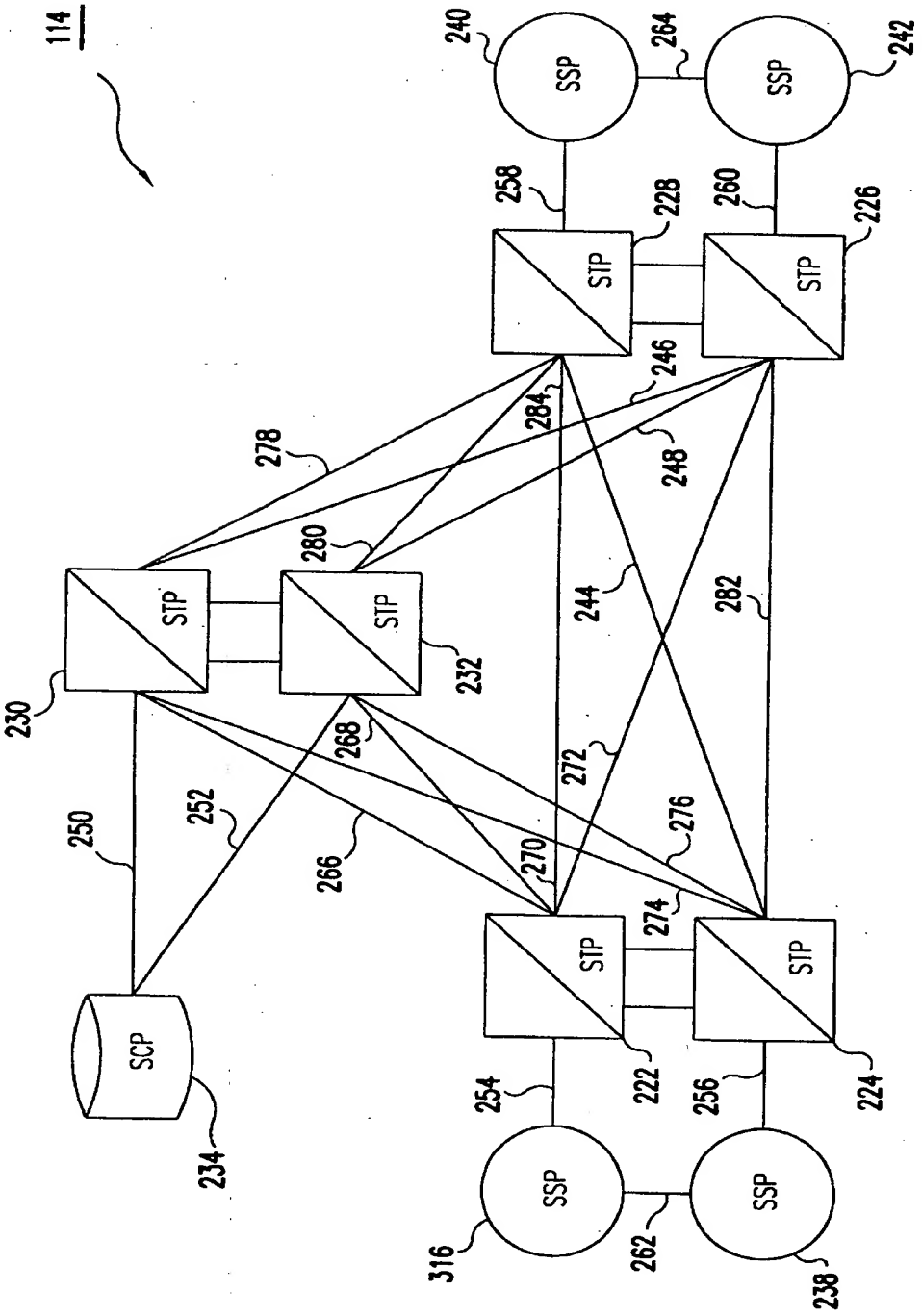

114
240
264
242
SSP
SSP
258
228
260
226
STP
STP
246
284
278
248
280
244
282
STP
STP
232
230
268
272
250
252
276
266
270
274
STP
STP
SCP
254
222
256
224
234
SSP
SSP
316
262
238

FIG.2B

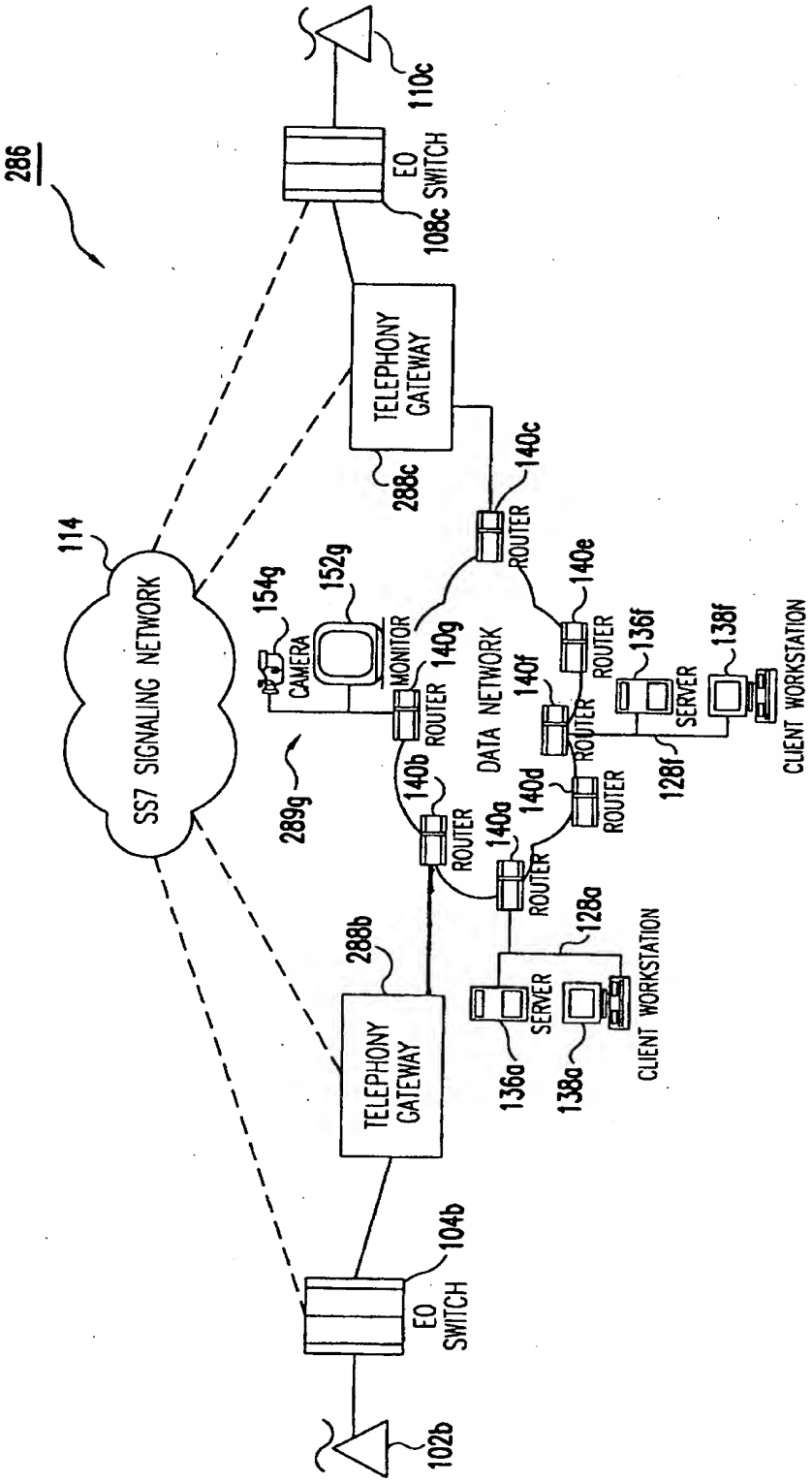

286
114
SS7 SIGNALING NETWORK
110c
EO SWITCH
108c
TELEPHONY GATEWAY
288c
140c
ROUTER
154g
CAMERA
152g
MONITOR
140g
ROUTER
140e
ROUTER
136f
SERVER
138f
CLIENT WORKSTATION
DATA NETWORK
140f
ROUTER
128f
289g
140b
ROUTER
140d
ROUTER
140a
ROUTER
128a
288b
SERVER
CLIENT WORKSTATION
136a
138a
TELEPHONY GATEWAY
104b
EO SWITCH
102b

FIG.2C

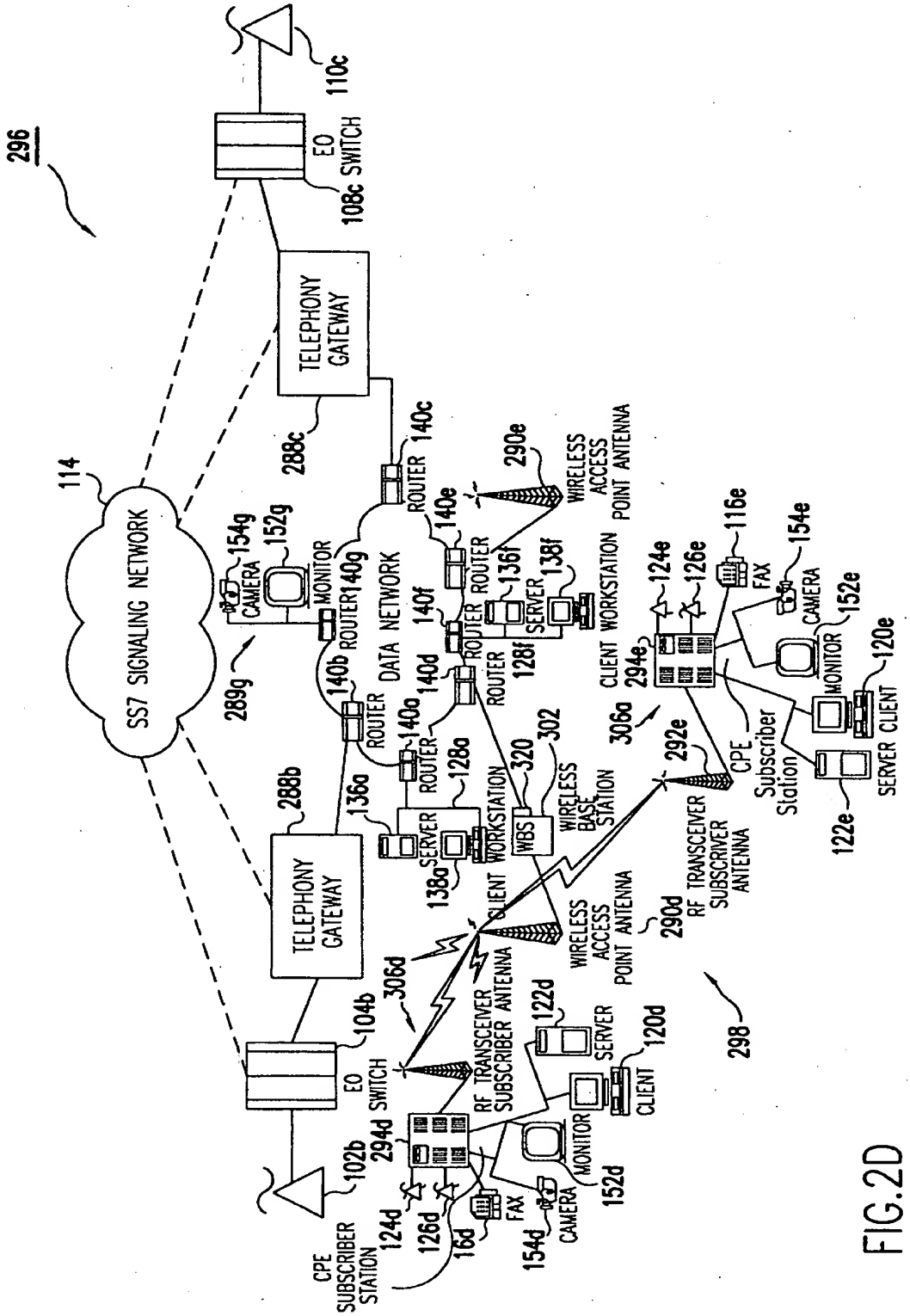

296
110c
EO SWITCH
108c
TELEPHONY GATEWAY
288c
114
SS7 SIGNALING NETWORK
ROUTER 140c
290e
WIRELESS ACCESS POINT ANTENNA
154g
152g
CAMERA
MONITOR
ROUTER 140g
140e
ROUTER
136f
SERVER
138f
124e
126e
116e
154e
FAX
CAMERA
152e
289g
140b
ROUTER
DATA NETWORK
140f
ROUTER
ROUTER
128f
CLIENT WORKSTATION
294e
MONITOR
120e
140a
ROUTER
140d
306a
292e
CPE Subscriber Station
SERVER CLIENT
288b
136a
ROUTER
128a
320
302
WIRELESS BASE STATION
122e
SERVER
WORKSTATION
WBS
138a
CLIENT
TELEPHONY GATEWAY
WIRELESS ACCESS POINT ANTENNA
290d
RF TRANSCEIVER SUBSCRIBER ANTENNA
306d
RF TRANSCEIVER SUBSCRIBER ANTENNA
122d
SERVER
120d
104b
EO SWITCH
CLIENT
298
294d
MONITOR
152d
102b
FAX
CAMERA
124d
126d
16d
154d
CPE SUBSCRIBER STATION

FIG.2D

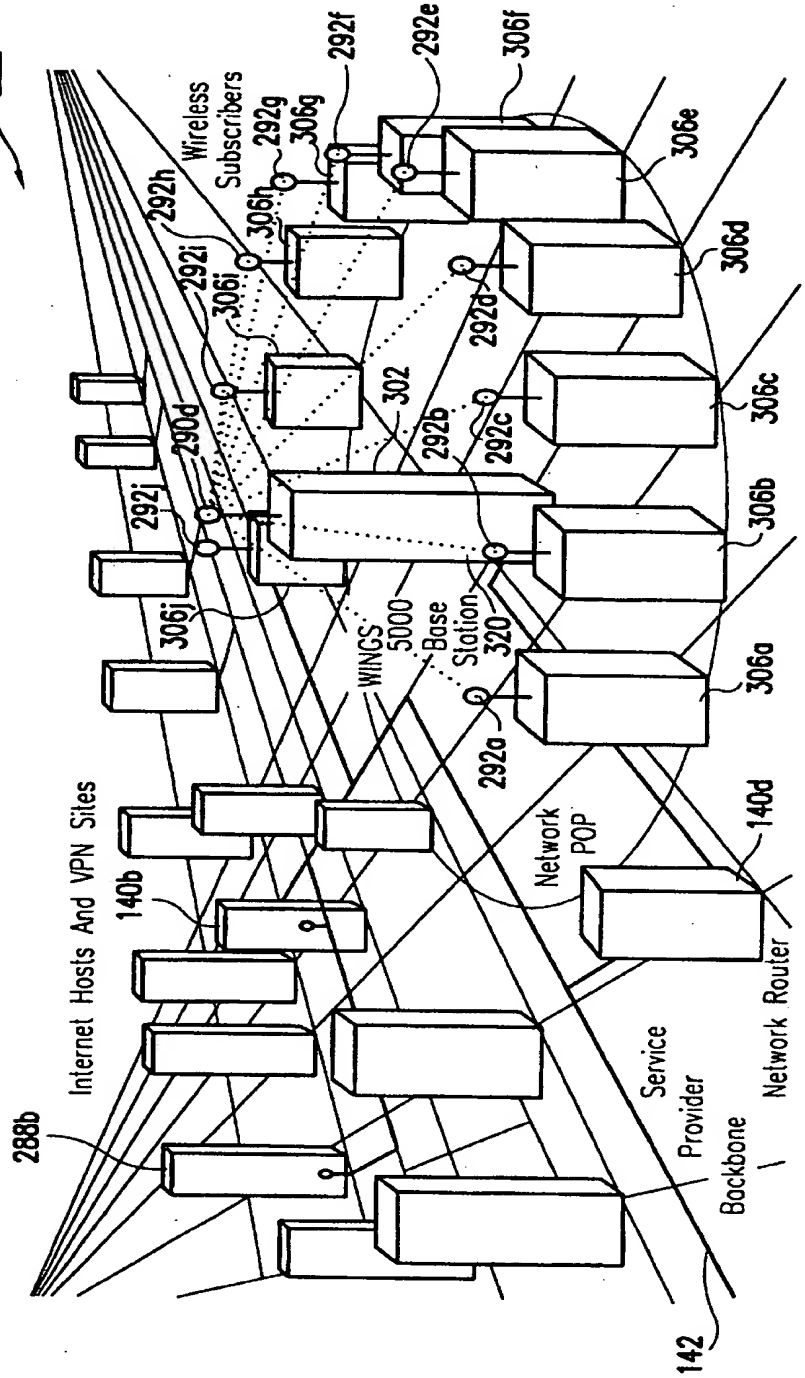

300
Wireless Subscribers
292f
292e
306f
306e
292g
306g
292h
306h
306d
292i
306i
292d
302
306c
290d
292b
292c
292j
306b
306j
WINGS 5000 Base Station
320
306a
292a
140d
Network POP
140b
Internet Hosts And VPN Sites
288b
Service Provider Backbone
Network Router
142

FIG.3A

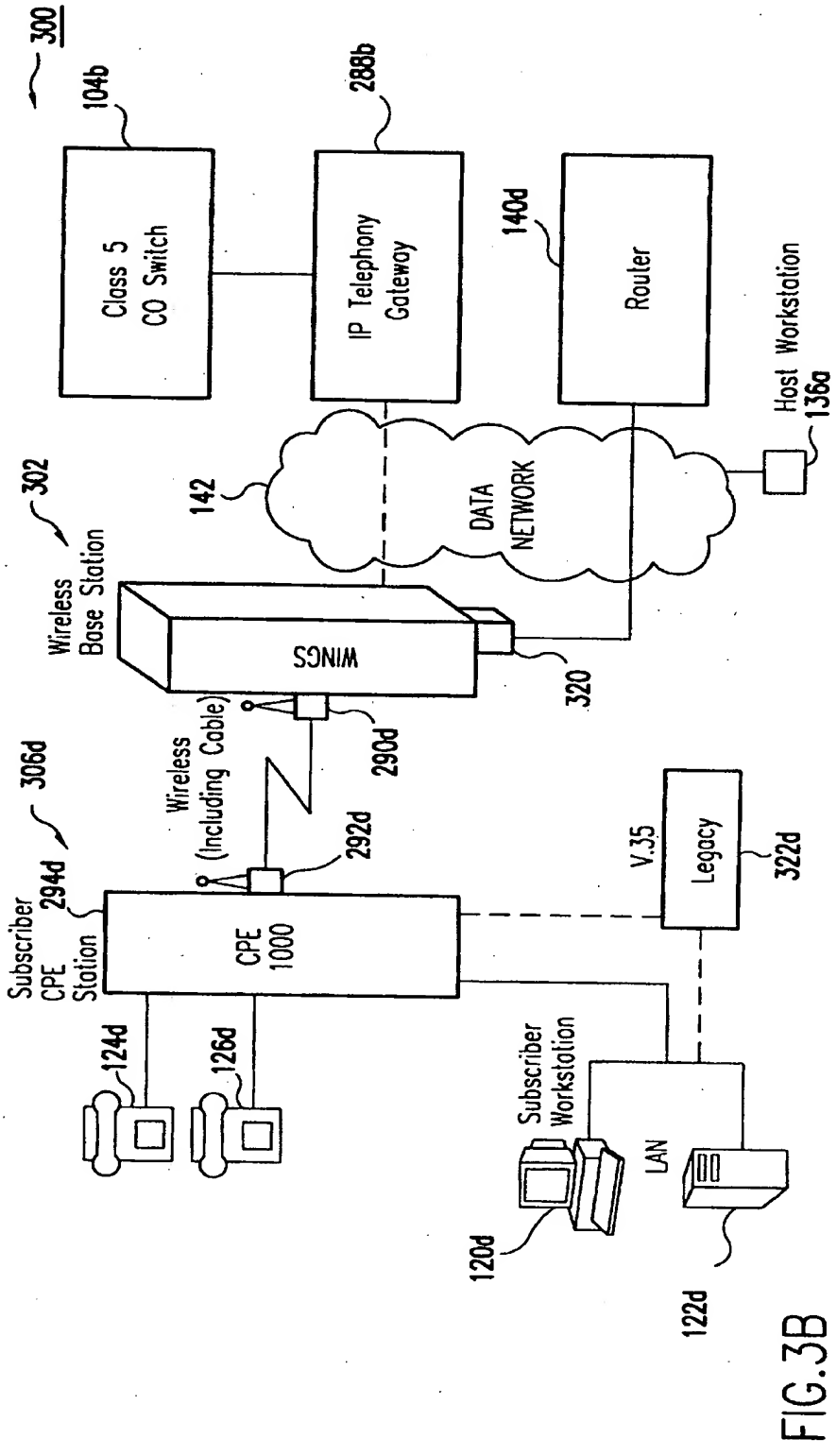

300
104b
Class 5 CO Switch
288b
IP Telephony Gateway
140d
Router
Host Workstation
136a
142
DATA NETWORK
302
Wireless Base Station
WINCS
320
290d
Wireless (Including Cable)
306d
292d
294d
Subscriber CPE Station
CPE 1000
V.35
Legacy
322d
124d
126d
Subscriber Workstation
LAN
120d
122d

FIG.3B

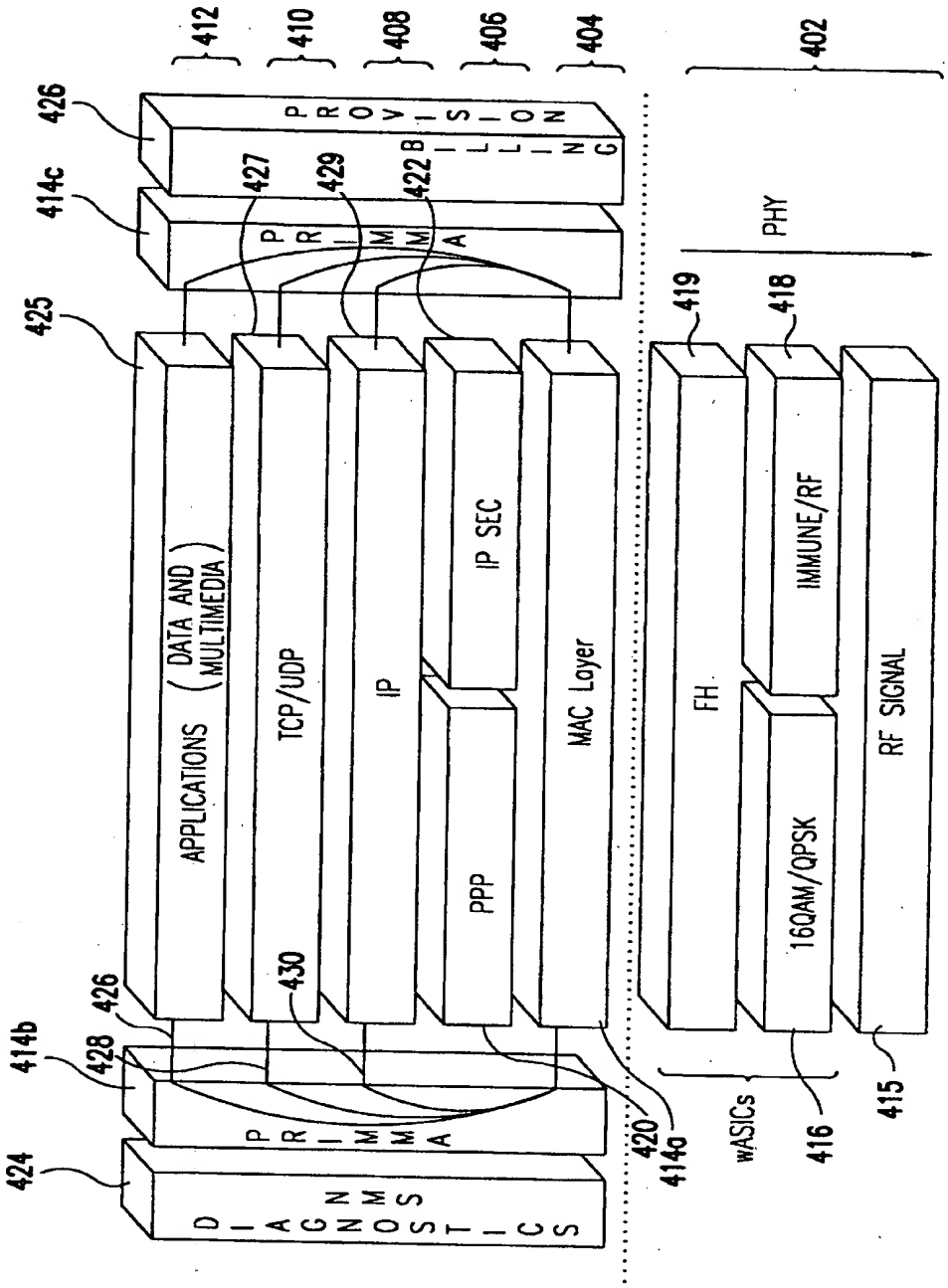
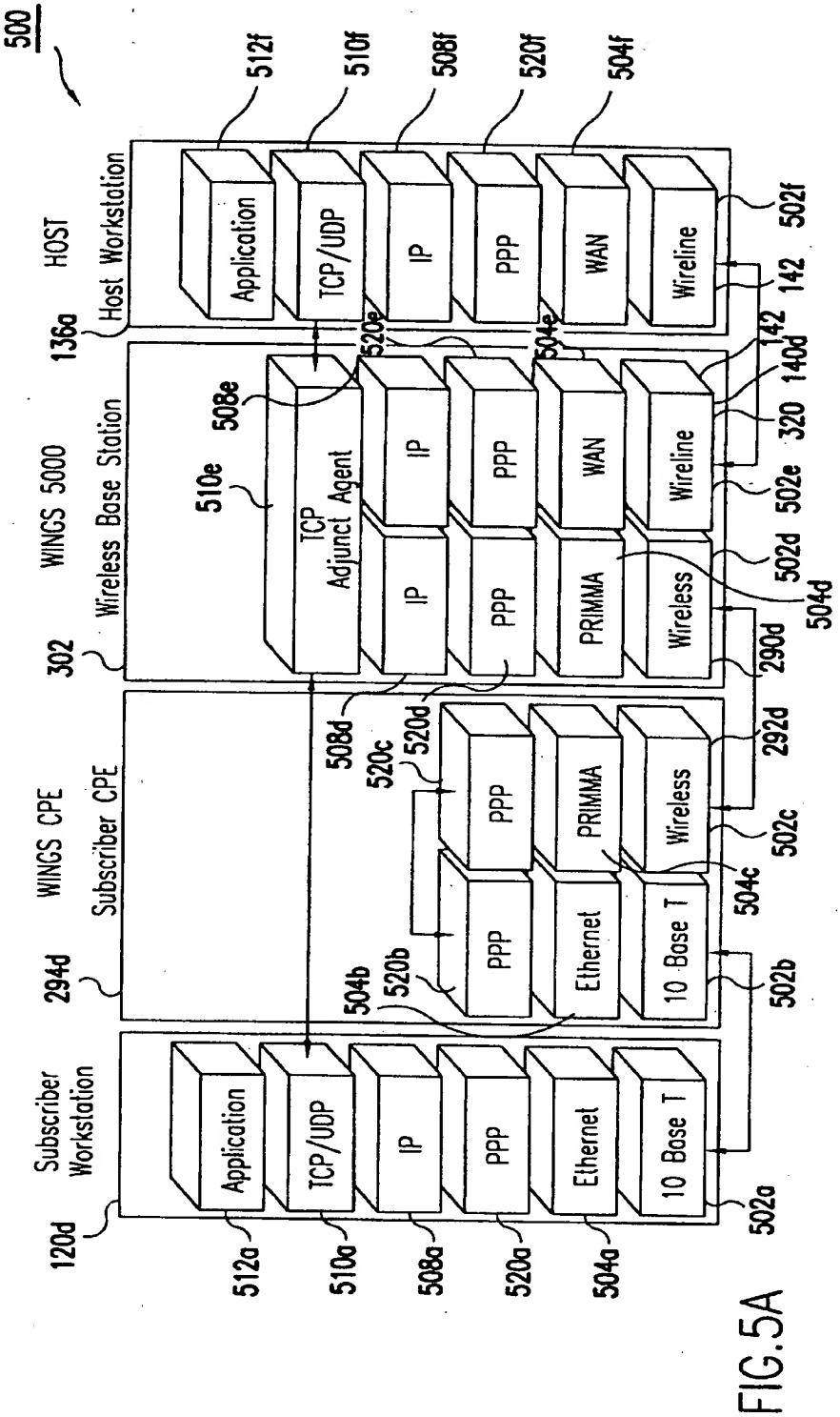

412
410
408
406
404
402
426
PROVISIONING
427
429
422
BILLING
414c
PRIMA
425
APPLICATIONS (DATA AND MULTIMEDIA)
TCP/UDP
IP
IP SEC
MAC Layer
PHY
419
418
FH
IMMUNE/RF
16QAM/QPSK
RF SIGNAL
430
426
414b
428
PRIMA
424
DIAGNOSTICS
420
414a
wASICs
416
415

FIG. 4


500
HOST
Host Workstation
136a
WINGS 5000
Wireless Base Station
302
WINGS CPE
Subscriber CPE
294d
Subscriber Workstation
120d
Application
TCP/UDP
IP
PPP
WAN
Wireline
TCP Adjunct Agent
PRIMMA
Wireless
Ethernet
10 Base T
512f
510f
508f
520f
504f
502f
142
140d
320
502e
502d
504d
290d
292d
502c
504c
502b
504b
520b
520c
520d
508d
508e
510e
512a
510a
508a
520a
504a
502a
FIG. 5A

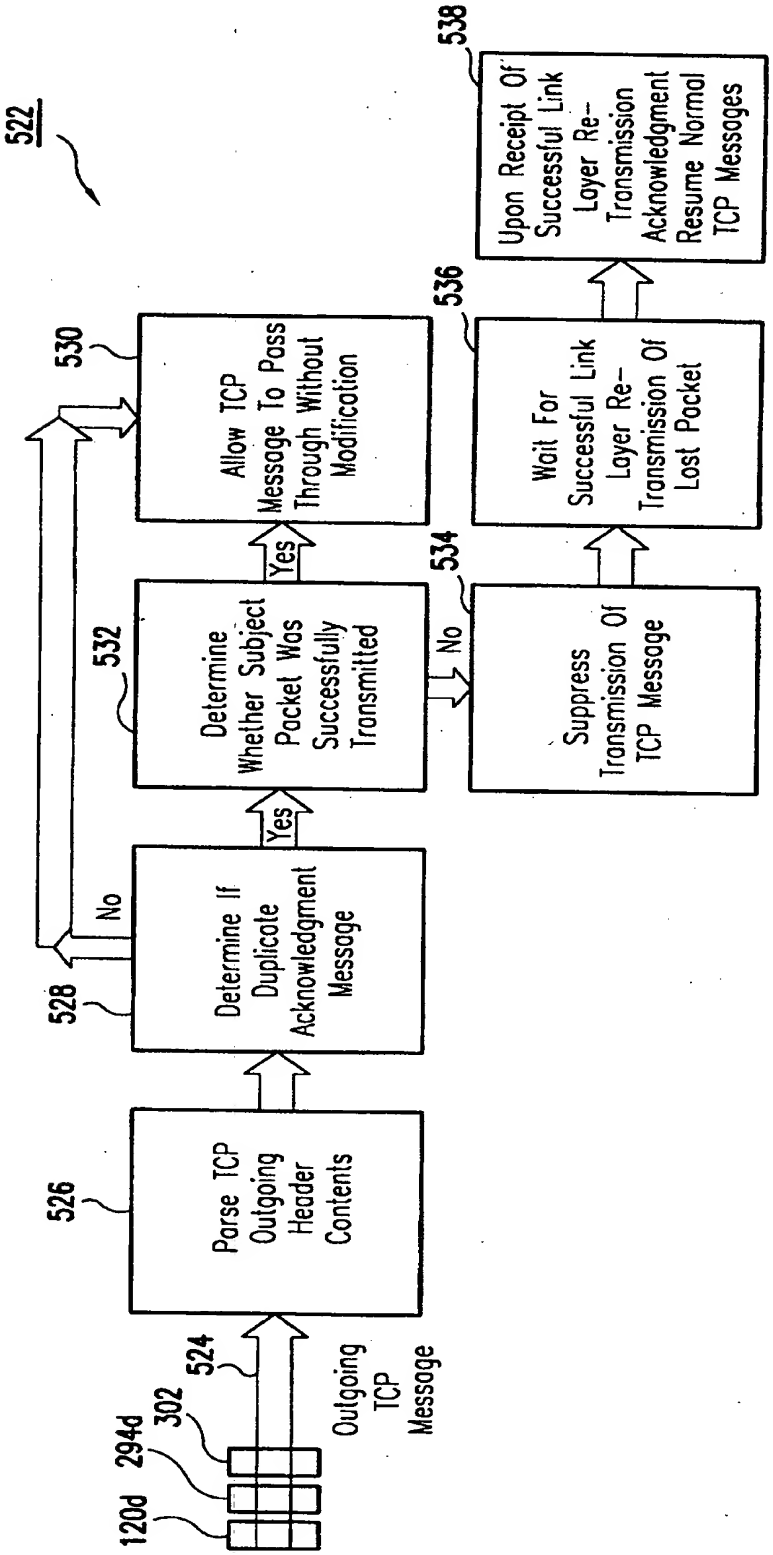

522
120d
294d
302
524
Outgoing TCP Message
526
Parse TCP Outgoing Header Contents
528
Determine If Duplicate Acknowledgment Message
No
Yes
532
Determine Whether Subject Packet Was Successfully Transmitted
Yes
No
530
Allow TCP Message To Pass Through Without Modification
534
Suppress Transmission Of TCP Message
536
Wait For Successful Link Layer Re-Transmission Of Lost Packet
538
Upon Receipt Of Successful Link Layer Re-Transmission Acknowledgment Resume Normal TCP Messages

FIG.5B

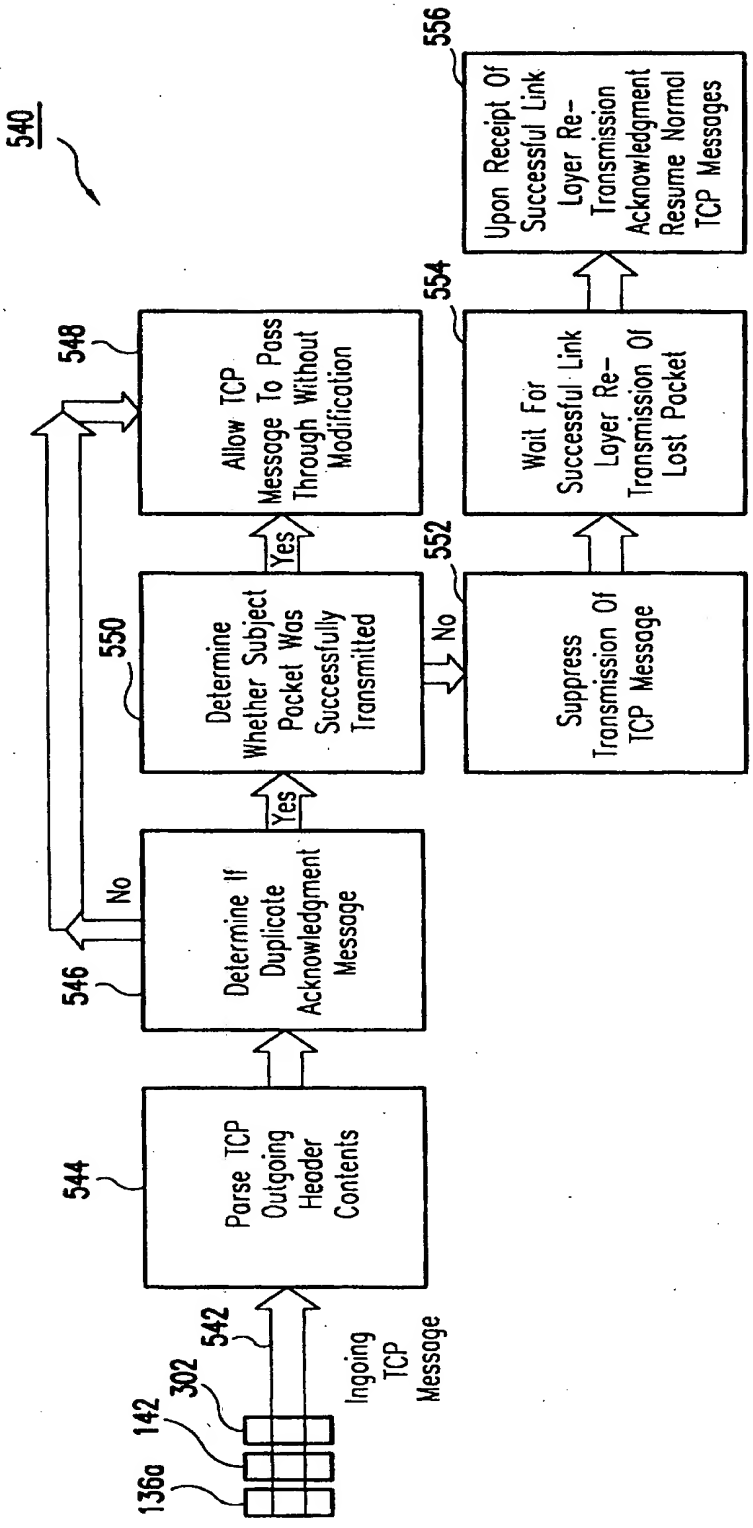

540
136a
142
302
542
Ingoing TCP Message
544
Parse TCP Outgoing Header Contents
546
Determine If Duplicate Acknowledgment Message
No
Yes
550
Determine Whether Subject Packet Was Successfully Transmitted
No
Yes
548
Allow TCP Message To Pass Through Without Modification
552
Suppress Transmission Of TCP Message
554
Wait For Successful Link Layer Re-Transmission Of Lost Packet
556
Upon Receipt Of Successful Link Layer Re-Transmission Acknowledgment Resume Normal TCP Messages

FIG.5C

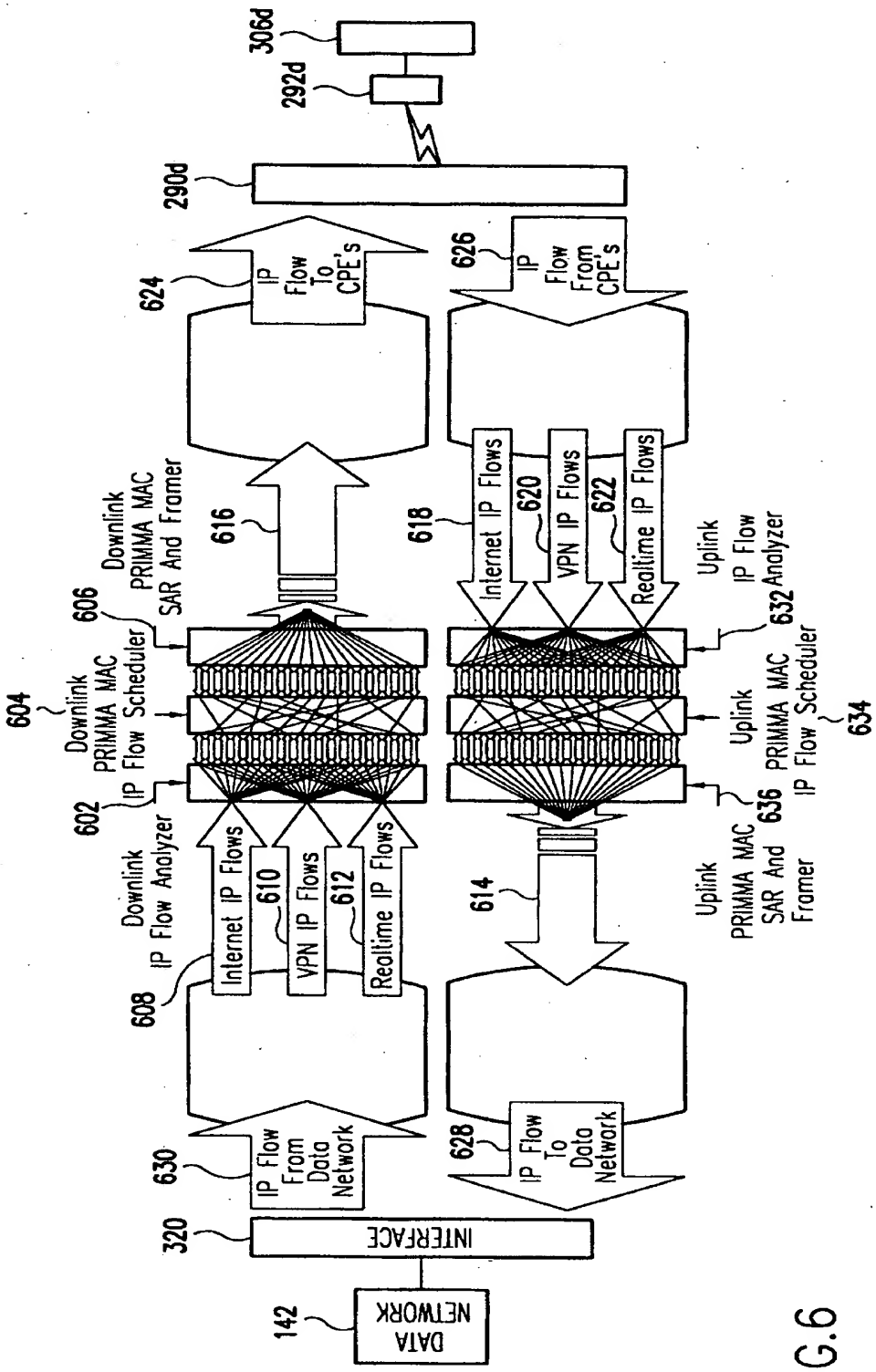

600
306d
292d
290d
624
IP Flow To CPE's
626
IP Flow From CPE's
616
618
Internet IP Flows
620
VPN IP Flows
622
Realtime IP Flows
Downlink PRIMMA MAC SAR And Framer
606
Downlink PRIMMA MAC IP Flow Scheduler
604
602
Downlink IP Flow Analyzer
608
Internet IP Flows
610
VPN IP Flows
612
Realtime IP Flows
614
Uplink IP Flow Analyzer
632
Uplink PRIMMA MAC IP Flow Scheduler
634
636
Uplink PRIMMA MAC SAR And Framer
630
IP Flow From Data Network
628
IP Flow To Data Network
320
INTERFACE
142
DATA NETWORK

FIG.6

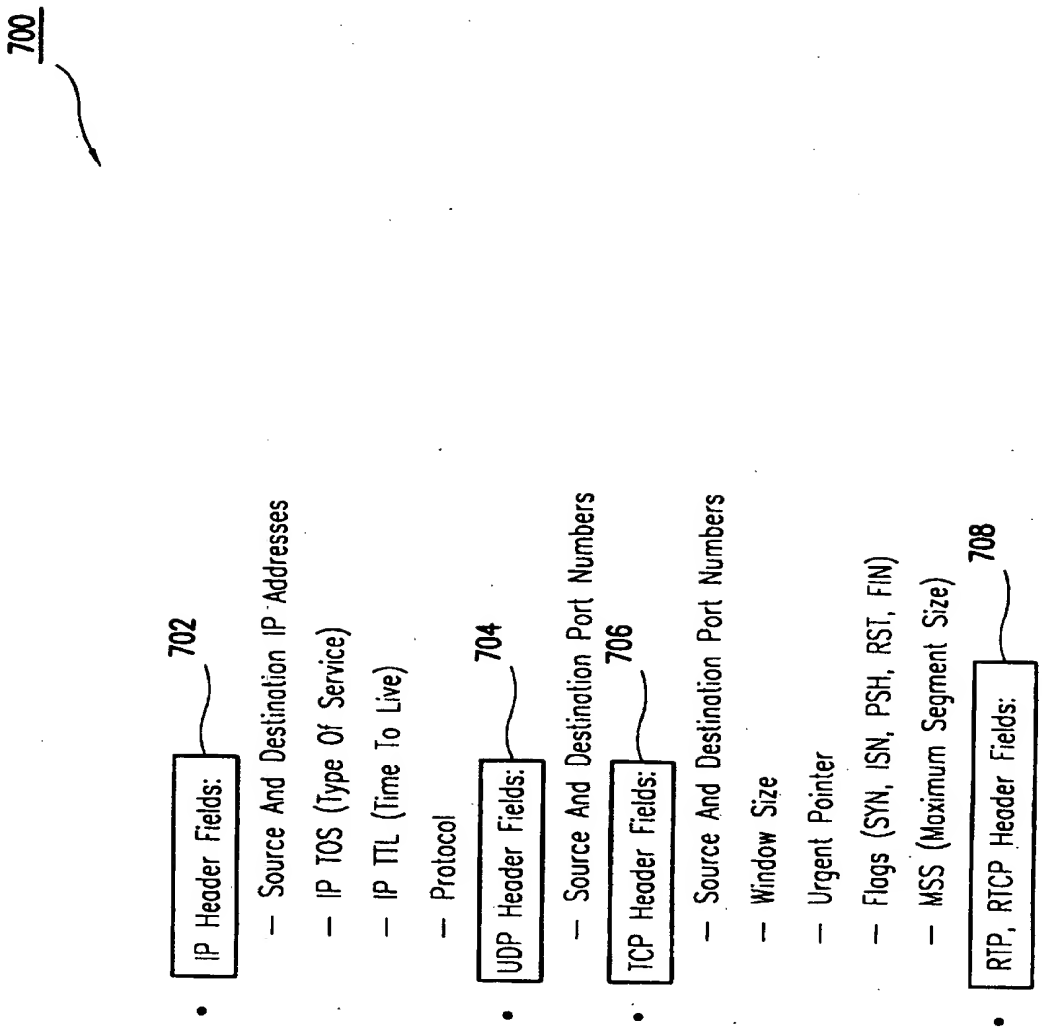

700
IP Header Fields:
702
– Source And Destination IP Addresses
– IP TOS (Type Of Service)
– IP TTL (Time To Live)
– Protocol
UDP Header Fields:
704
– Source And Destination Port Numbers
TCP Header Fields:
706
– Source And Destination Port Numbers
– Window Size
– Urgent Pointer
– Flags (SYN, ISN, PSH, RST, FIN)
– MSS (Maximum Segment Size)
RTP, RTCP Header Fields:
708

FIG. 7

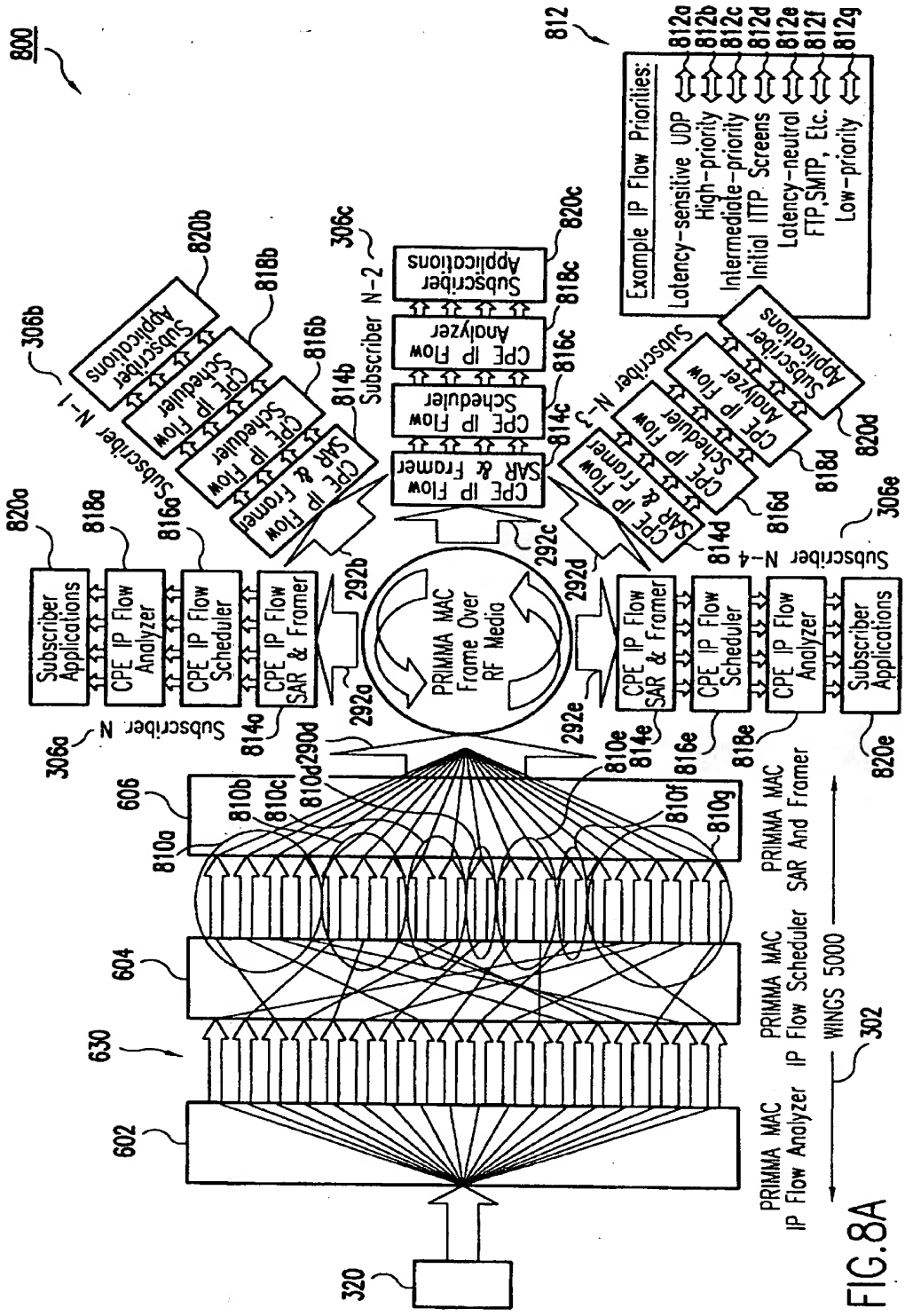

800
812
Example IP Flow Priorities:
812a Latency-sensitive UDP
812b High-priority
812c Intermediate-priority
812d Initial IITP Screens
812e Latency-neutral
812f FTP,SMTP, Etc.
812g Low-priority
306b Subscriber N-1
820b Subscriber Applications
818b CPE IP Flow Scheduler
816b CPE IP Flow Analyzer
814b CPE IP Flow SAR & Framer
306c Subscriber N-2
820c Subscriber Applications
818c CPE IP Flow Scheduler
816c CPE IP Flow Analyzer
814c CPE IP Flow SAR & Framer
306d Subscriber N-3
820d Subscriber Applications
818d CPE IP Flow Scheduler
816d CPE IP Flow Analyzer
814d CPE IP Flow SAR & Framer
306e Subscriber N-4
820a Subscriber Applications
818a CPE IP Flow Analyzer
816a CPE IP Flow Scheduler
814a CPE IP Flow SAR & Framer
306a Subscriber N
292a
292b
292c
292d
292e
PRIMMA MAC Frame Over RF Media
820e Subscriber Applications
818e CPE IP Flow Analyzer
816e CPE IP Flow Scheduler
814e CPE IP Flow SAR & Framer
810a
810b
810c
810d
810e
810f
810g
606
604
630
602
320
PRIMMA MAC IP Flow Analyzer
PRIMMA MAC IP Flow Scheduler
PRIMMA MAC SAR And Framer
WINGS 5000
302

FIG.8A

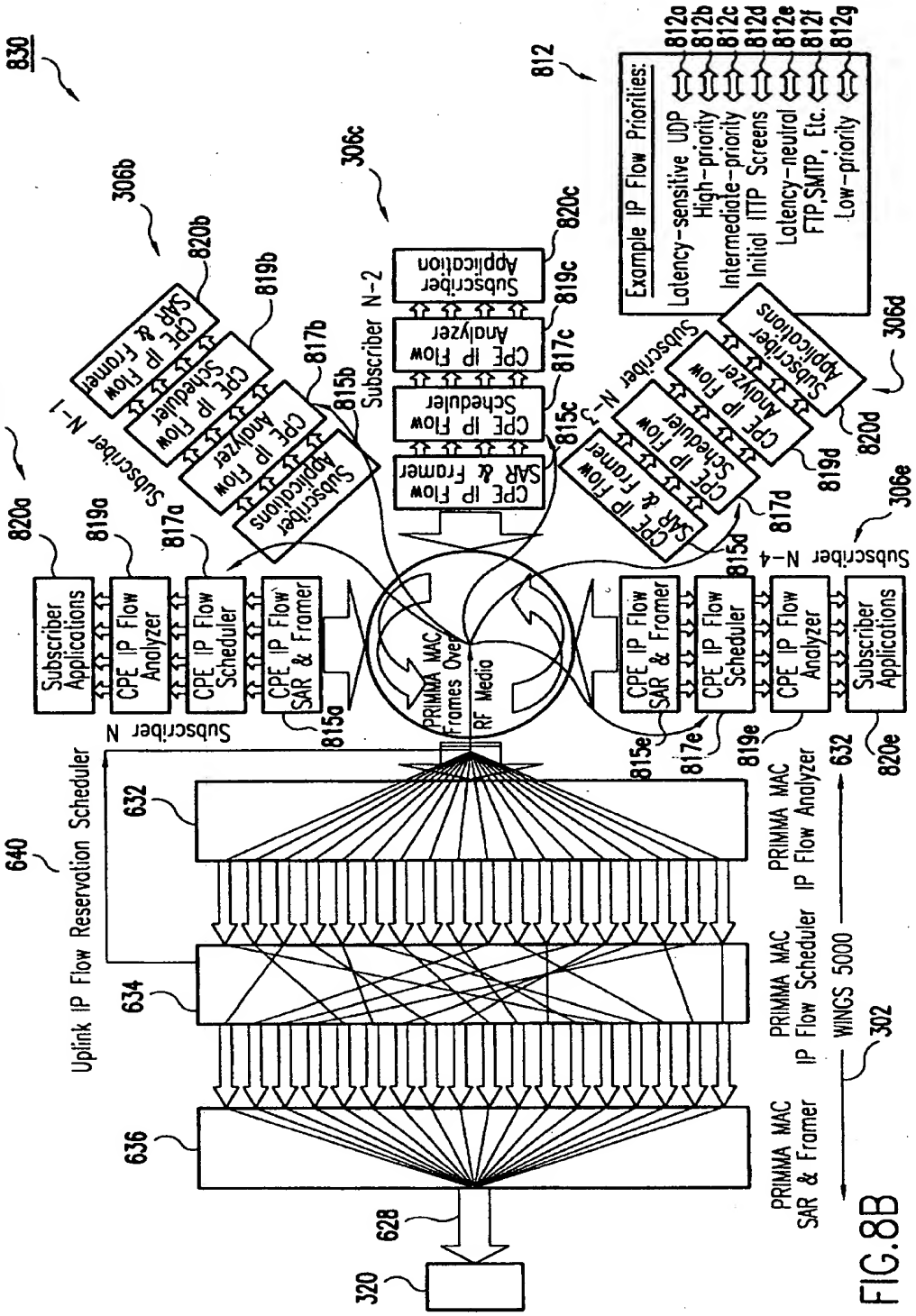

830
812
Example IP Flow Priorities:
812a Latency-sensitive UDP
812b High-priority
812c Intermediate-priority
812d Initial ITTP Screens
812e Latency-neutral
812f FTP,SMTP, Etc.
812g Low-priority
306a
306b
306c
306d
306e
Subscriber N-1
Subscriber N-2
Subscriber N-3
Subscriber N-4
Subscriber N
820a
820b
820c
820d
820e
819a
819b
819c
819d
819e
817a
817b
817c
817d
817e
815a
815b
815c
815d
815e
Subscriber Applications
CPE IP Flow Analyzer
CPE IP Flow Scheduler
CPE IP Flow SAR & Framer
PRIMA MAC Frames Over RF Media
640
Uplink IP Flow Reservation Scheduler
632
634
636
628
320
PRIMA MAC SAR & Framer
PRIMA MAC IP Flow Scheduler
PRIMA MAC IP Flow Analyzer
WINGS 5000
302

FIG.8B

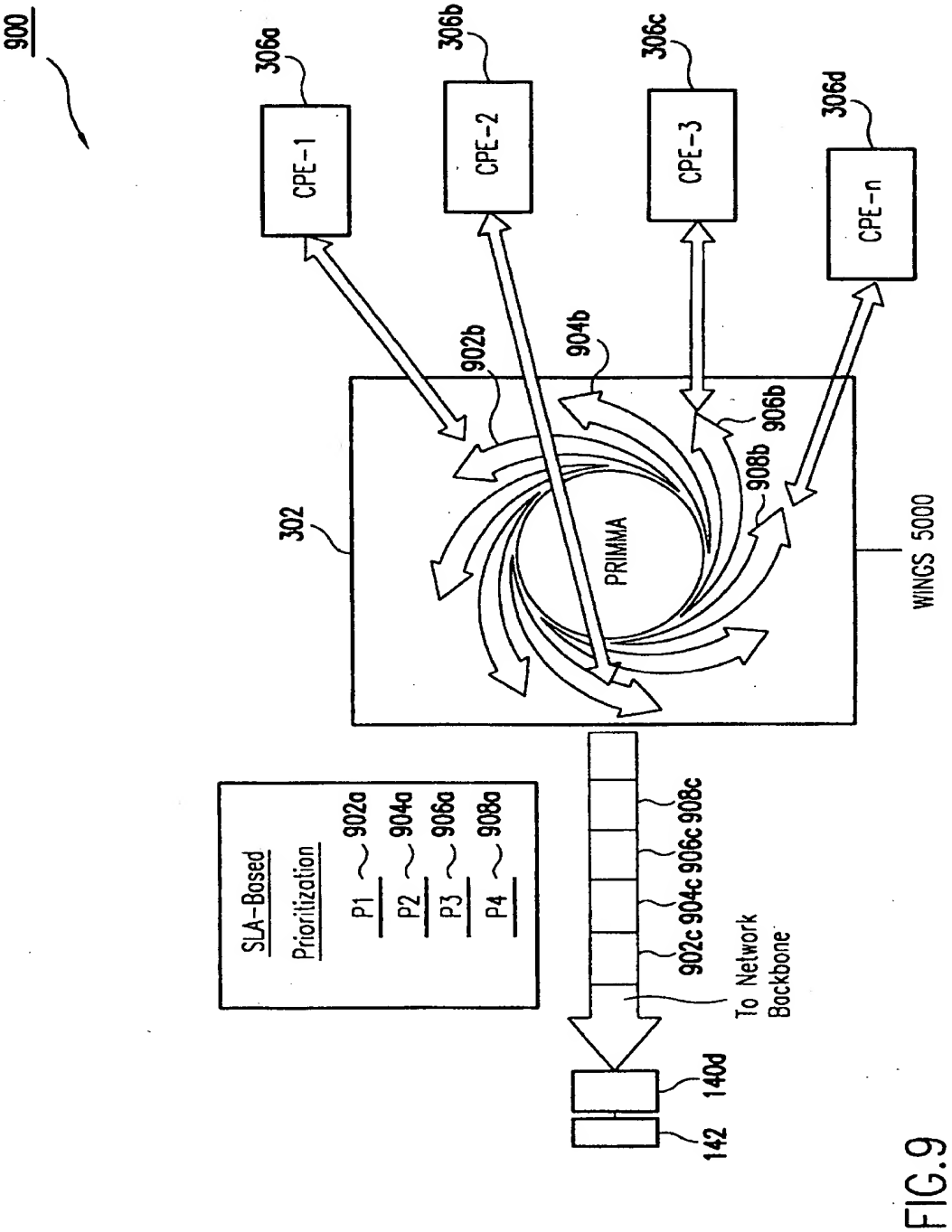

900
306a
CPE-1
306b
CPE-2
306c
CPE-3
306d
CPE-n
902b
904b
906b
908b
302
PRIMMA
WINGS 5000
SLA-Based
Prioritization
P1 902a
P2 904a
P3 906a
P4 908a
902c 904c 906c 908c
To Network
Backbone
140d
142

FIG.9

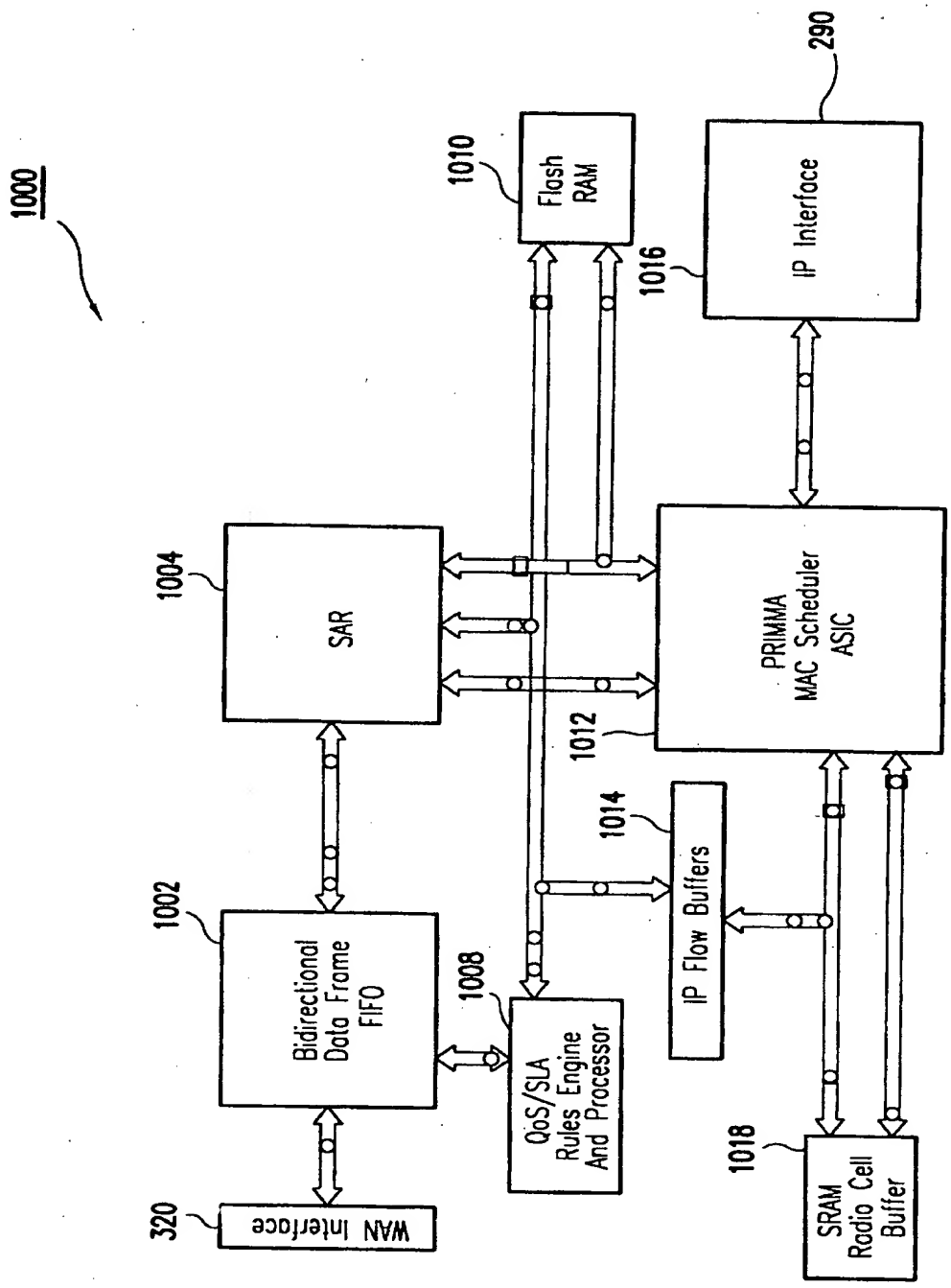

1000
1010
Flash RAM
290
IP Interface
1016
1004
SAR
PRIMMA MAC Scheduler ASIC
1012
1014
IP Flow Buffers
1002
Bidirectional Data Frame FIFO
1008
QoS/SLA Rules Engine And Processor
1018
SRAM Radio Cell Buffer
320
WAN Interface

FIG. 10

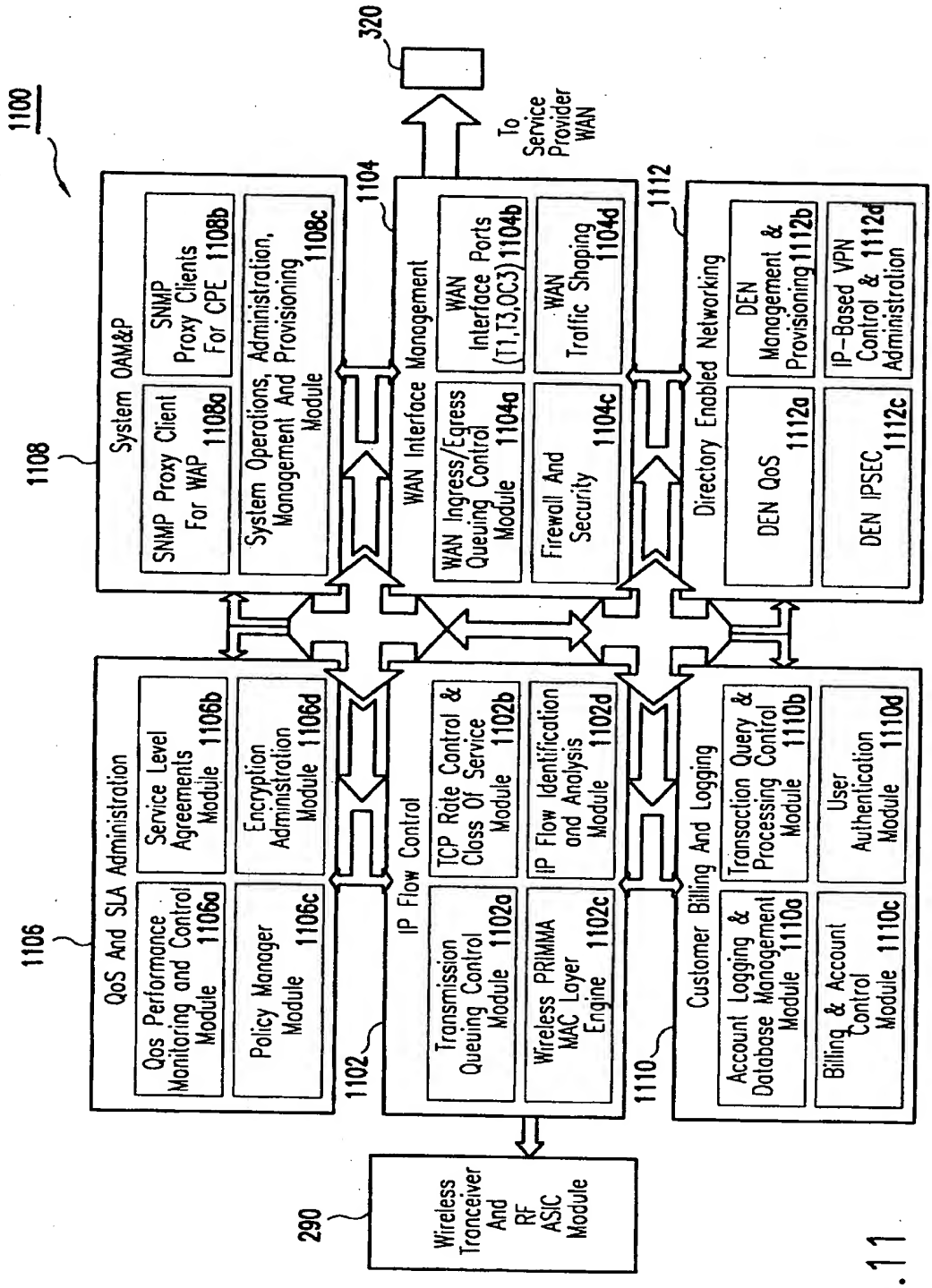

1100
320
To Service Provider WAN
1104
1112
1108
System OAM&P
SNMP Proxy Client For WAP 1108a
SNMP Proxy Clients For CPE 1108b
System Operations, Administration, Management And Provisioning Module 1108c
WAN Interface Management
WAN Ingress/Egress Queuing Control Module 1104a
WAN Interface Ports (T1,T3,OC3) 1104b
Firewall And Security 1104c
WAN Traffic Shaping 1104d
Directory Enabled Networking
DEN QoS 1112a
DEN Management & Provisioning 1112b
DEN IPSEC 1112c
IP-Based VPN Control & Administration 1112d
1106
QoS And SLA Administration
Qos Performance Monitoring and Control Module 1106a
Service Level Agreements Module 1106b
Policy Manager Module 1106c
Encryption Administration Module 1106d
1102
IP Flow Control
Transmission Queuing Control Module 1102a
TCP Rate Control & Class Of Service Module 1102b
Wireless PRIMA MAC Layer Engine 1102c
IP Flow Identification and Analysis Module 1102d
1110
Customer Billing And Logging
Account Logging & Database Management Module 1110a
Billing & Account Control Module 1110c
Transaction Query & Processing Control Module 1110b
User Authentication Module 1110d
290
Wireless Tranceiver And RF ASIC Module

FIG. 11

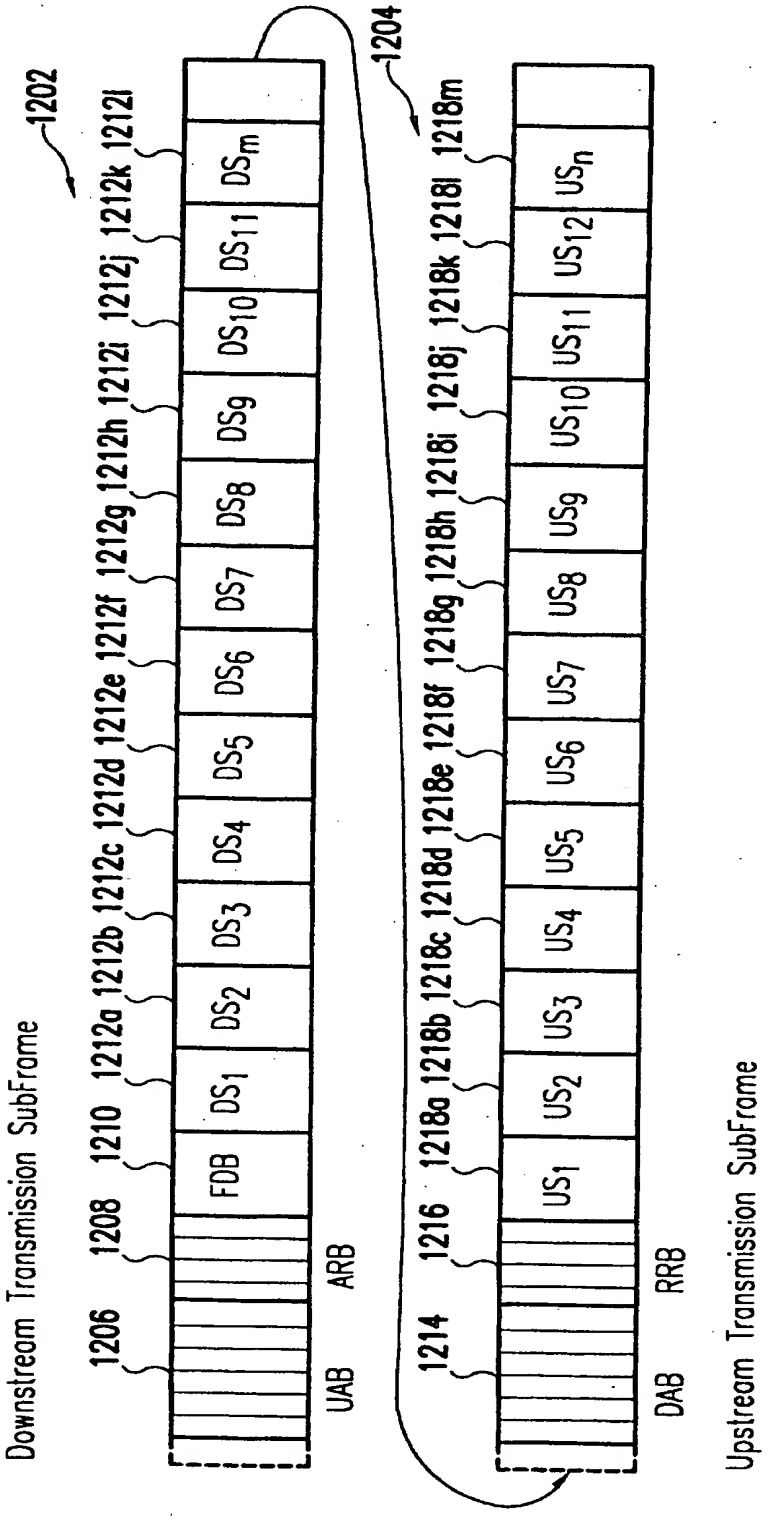

1202
1204
Downstream Transmission SubFrame
Upstream Transmission SubFrame
1206
1208
1210
1212a
1212b
1212c
1212d
1212e
1212f
1212g
1212h
1212i
1212j
1212k
1212l
1214
1216
1218a
1218b
1218c
1218d
1218e
1218f
1218g
1218h
1218i
1218j
1218k
1218l
1218m
FDB
DS1
DS2
DS3
DS4
DS5
DS6
DS7
DS8
DS9
DS10
DS11
DSm
UAB
ARB
US1
US2
US3
US4
US5
US6
US7
US8
US9
US10
US11
US12
USn
DAB
RRB

FIG. 12A

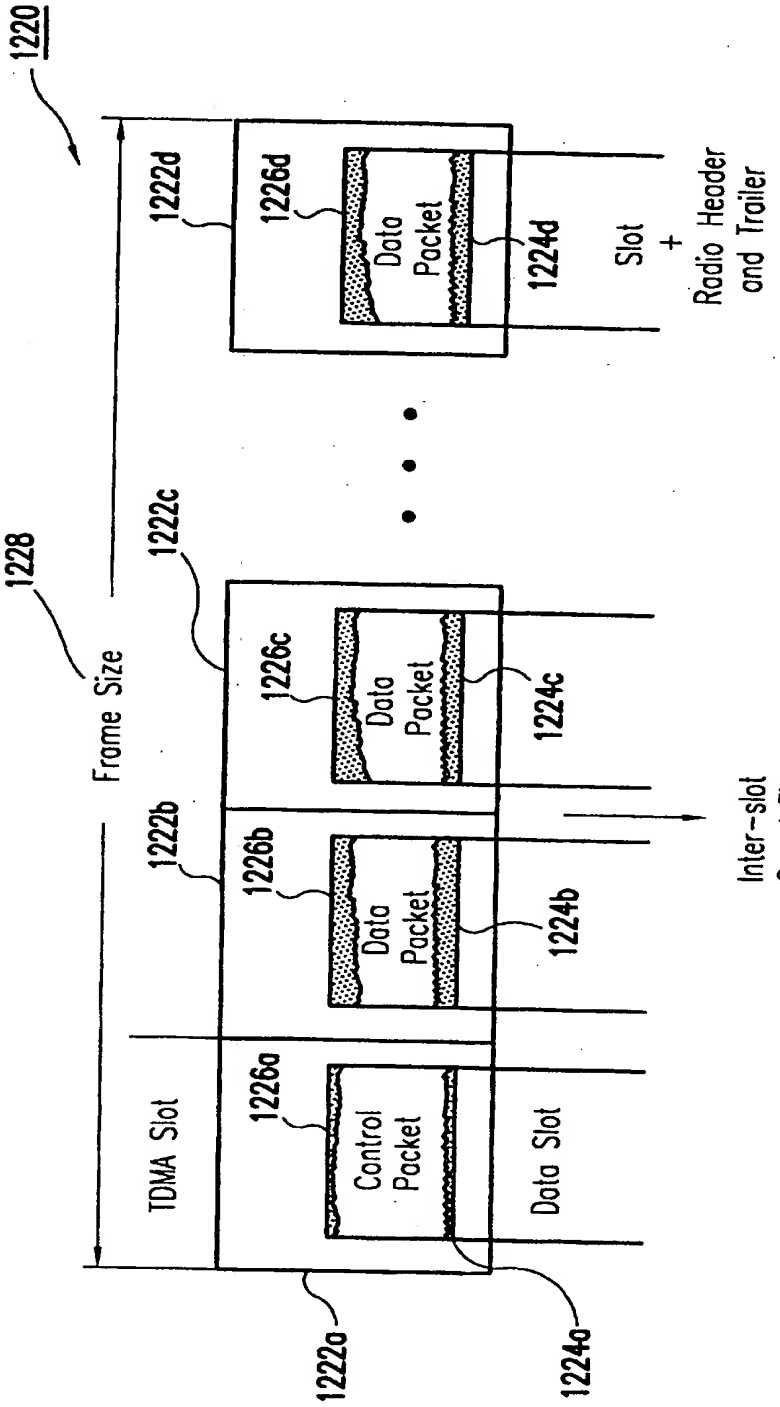

1220
1222d
1226d
Data Packet
1224d
Slot + Radio Header and Trailer
1228
Frame Size
1222c
1226c
Data Packet
1224c
1222b
1226b
Data Packet
1224b
Inter-slot Guard Time
1229
TDMA Slot
1226a
Control Packet
Data Slot
1222a
1224a

FIG.12B

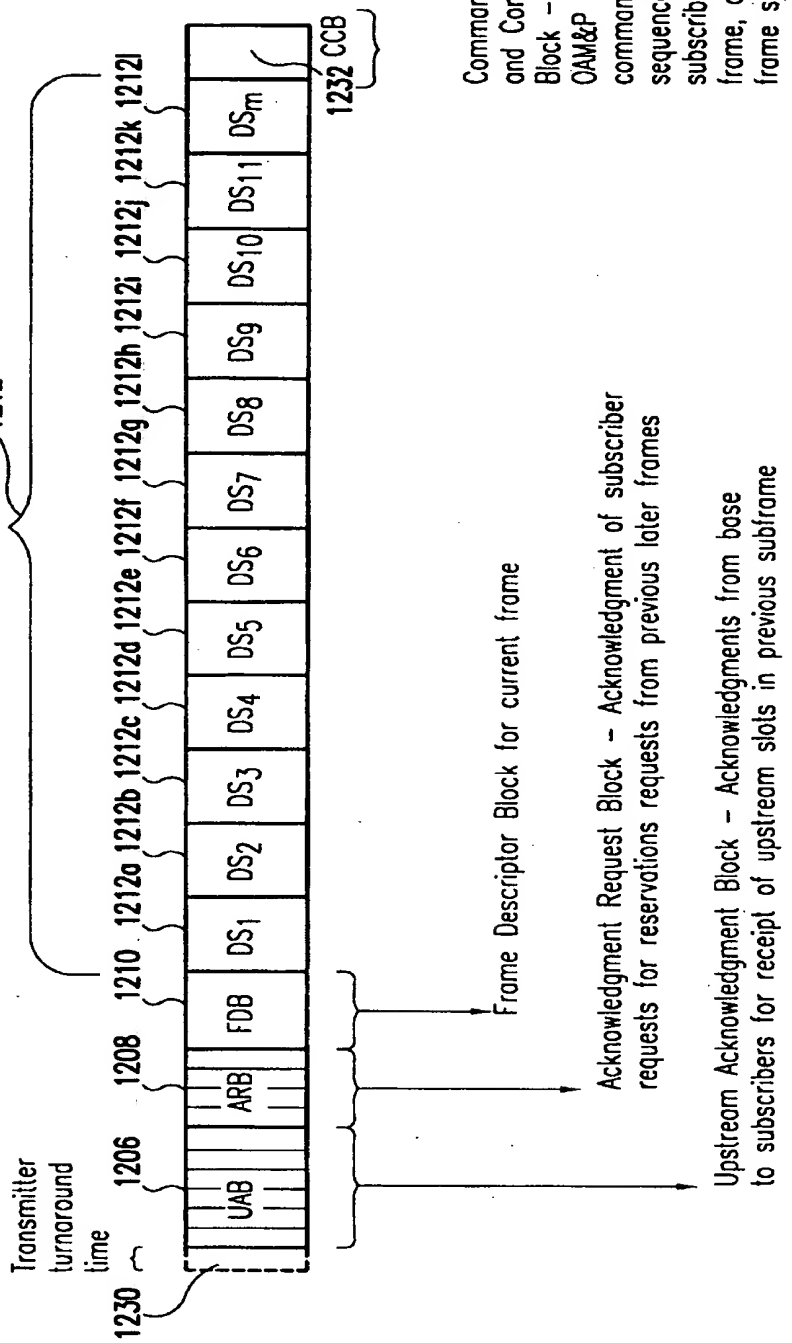

Downstream slots transmissions
(variable number per frame up to 16)
1202
1212
1210
1212a
1212b
1212c
1212d
1212e
1212f
1212g
1212h
1212i
1212j
1212k
1212l
1208
1206
1230
Transmitter turnaround time
UAB
ARB
FDB
DS1
DS2
DS3
DS4
DS5
DS6
DS7
DS8
DS9
DS10
DS11
DSm
1232 CCB
Command and Control Block - OAM&P commands sequenced by subscriber per frame, and frame sync
Frame Descriptor Block for current frame
Acknowledgment Request Block - Acknowledgment of subscriber requests for reservations requests from previous later frames
Upstream Acknowledgment Block - Acknowledgments from base to subscribers for receipt of upstream slots in previous subframe

FIG.12C

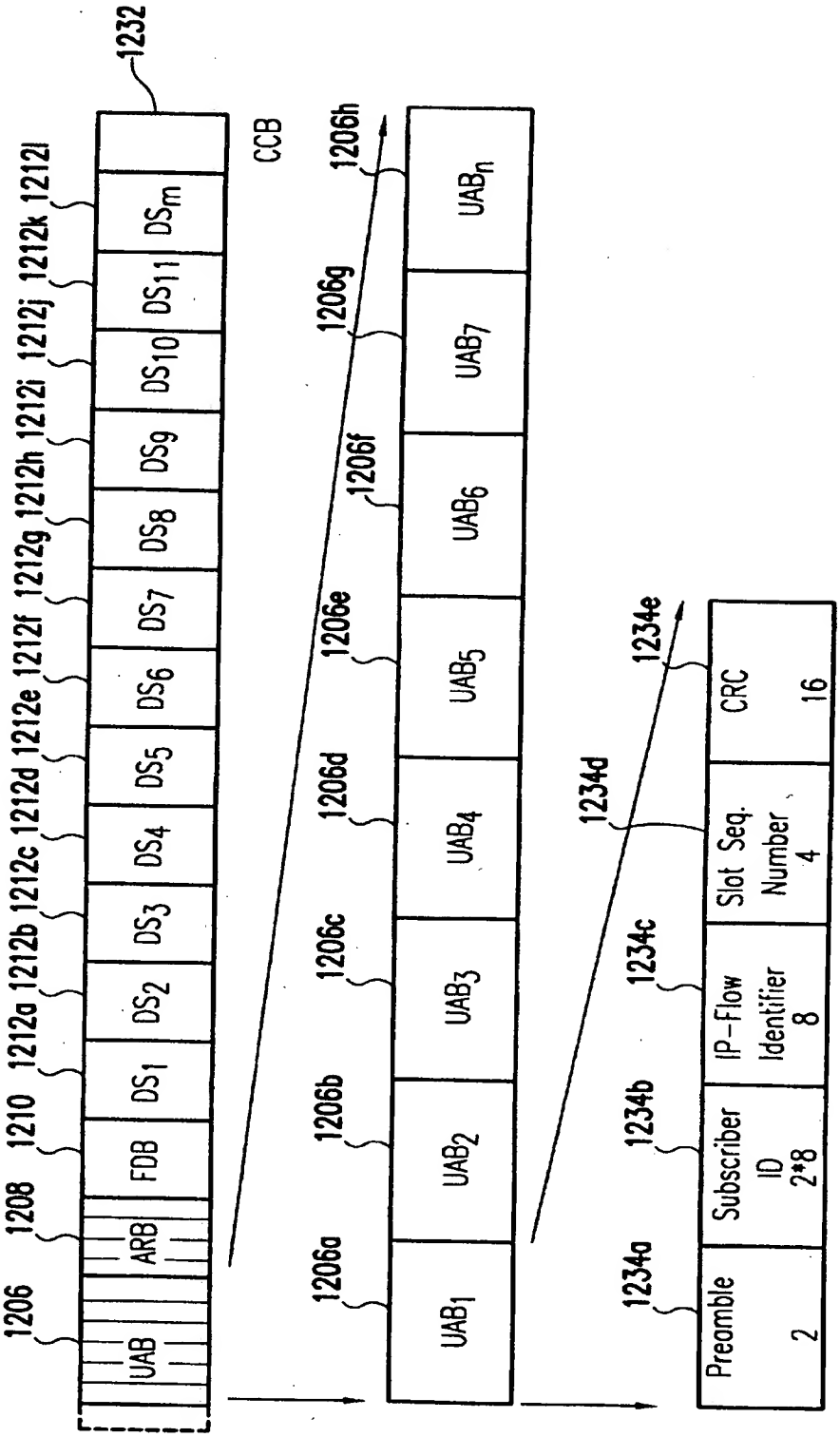

1202
1232
CCB
1212l
1212k
1212j
1212i
1212h
1212g
1212f
1212e
1212d
1212c
1212b
1212a
1210
1208
1206
1206h
1206g
1206f
1206e
1206d
1206c
1206b
1206a
1234e
1234d
1234c
1234b
1234a
UAB
ARB
FDB
DS1
DS2
DS3
DS4
DS5
DS6
DS7
DS8
DS9
DS10
DS11
DSm
UAB1
UAB2
UAB3
UAB4
UAB5
UAB6
UAB7
UABn
Preomble 2
Subscriber ID 2*8
IP-Flow Identifier 8
Slot Seq. Number 4
CRC 16

FIG. 12D

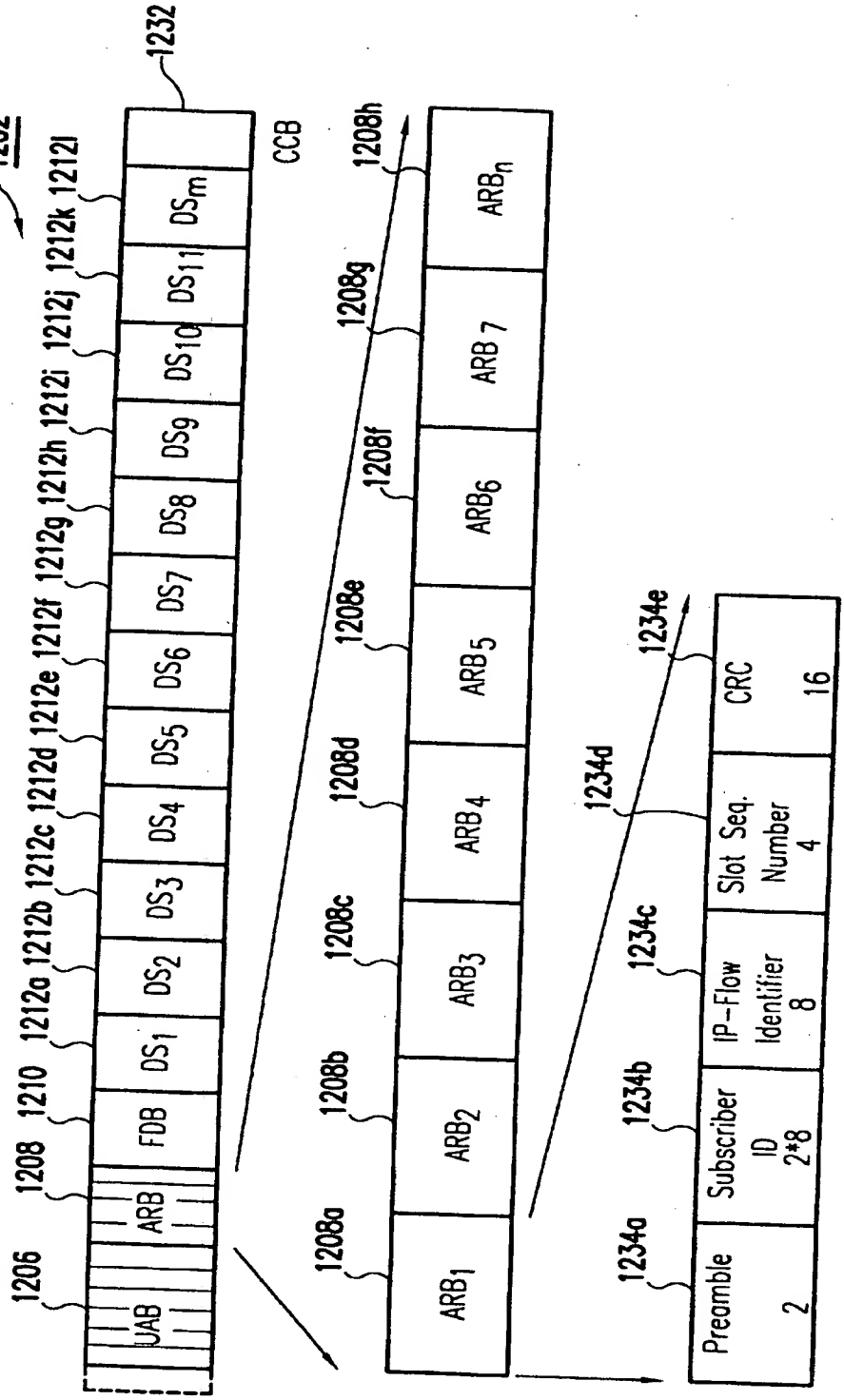

1202
1232
CCB
1206
UAB
1208
ARB
1210
FDB
1212a
DS1
1212b
DS2
1212c
DS3
1212d
DS4
1212e
DS5
1212f
DS6
1212g
DS7
1212h
DS8
1212i
DS9
1212j
DS10
1212k
DS11
1212l
DSm
1208a
ARB1
1208b
ARB2
1208c
ARB3
1208d
ARB4
1208e
ARB5
1208f
ARB6
1208g
ARB7
1208h
ARBn
1234a
Preamble
2
1234b
Subscriber ID
2*8
1234c
IP-Flow Identifier
8
1234d
Slot Seq. Number
4
1234e
CRC
16

FIG. 12E

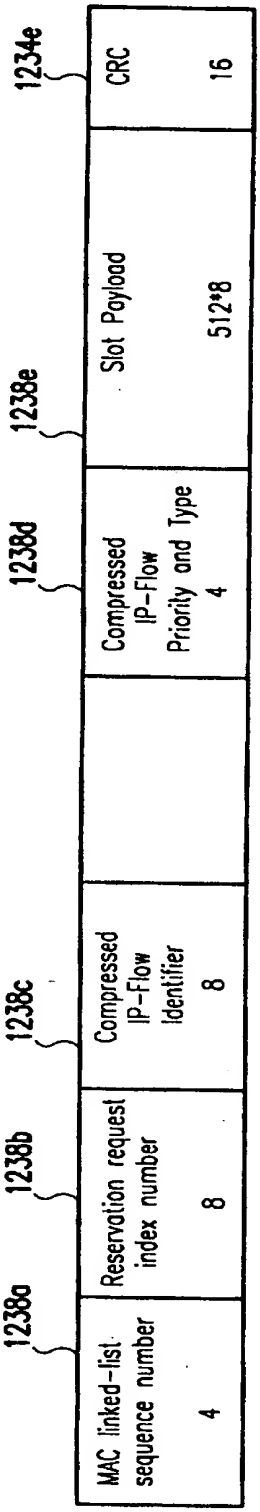

1238a
MAC linked-list sequence number
4
1238b
Reservation request index number
8
1238c
Compressed IP-Flow Identifier
8
1238d
Compressed IP-Flow Priority and Type
4
1238e
Slot Payload
512*8
1234e
CRC
16

FIG. 12G

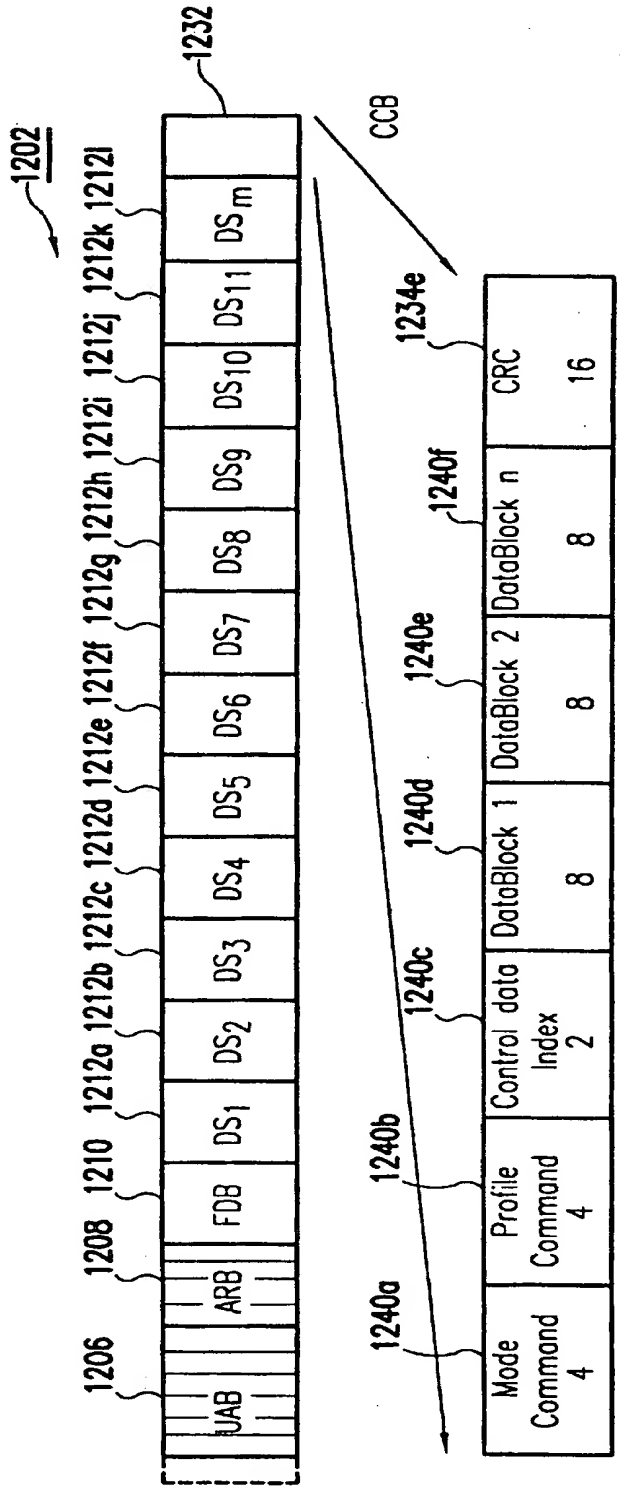

1202
1232
CCB
1206
UAB
1208
ARB
1210
FDB
1212a DS1
1212b DS2
1212c DS3
1212d DS4
1212e DS5
1212f DS6
1212g DS7
1212h DS8
1212i DS9
1212j DS10
1212k DS11
1212l DSm
1234e
CRC
16
1240f
DataBlock n
8
1240e
DataBlock 2
8
1240d
DataBlock 1
8
1240c
Control data
Index
2
1240b
Profile
Command
4
1240a
Mode
Command
4

FIG. 12H

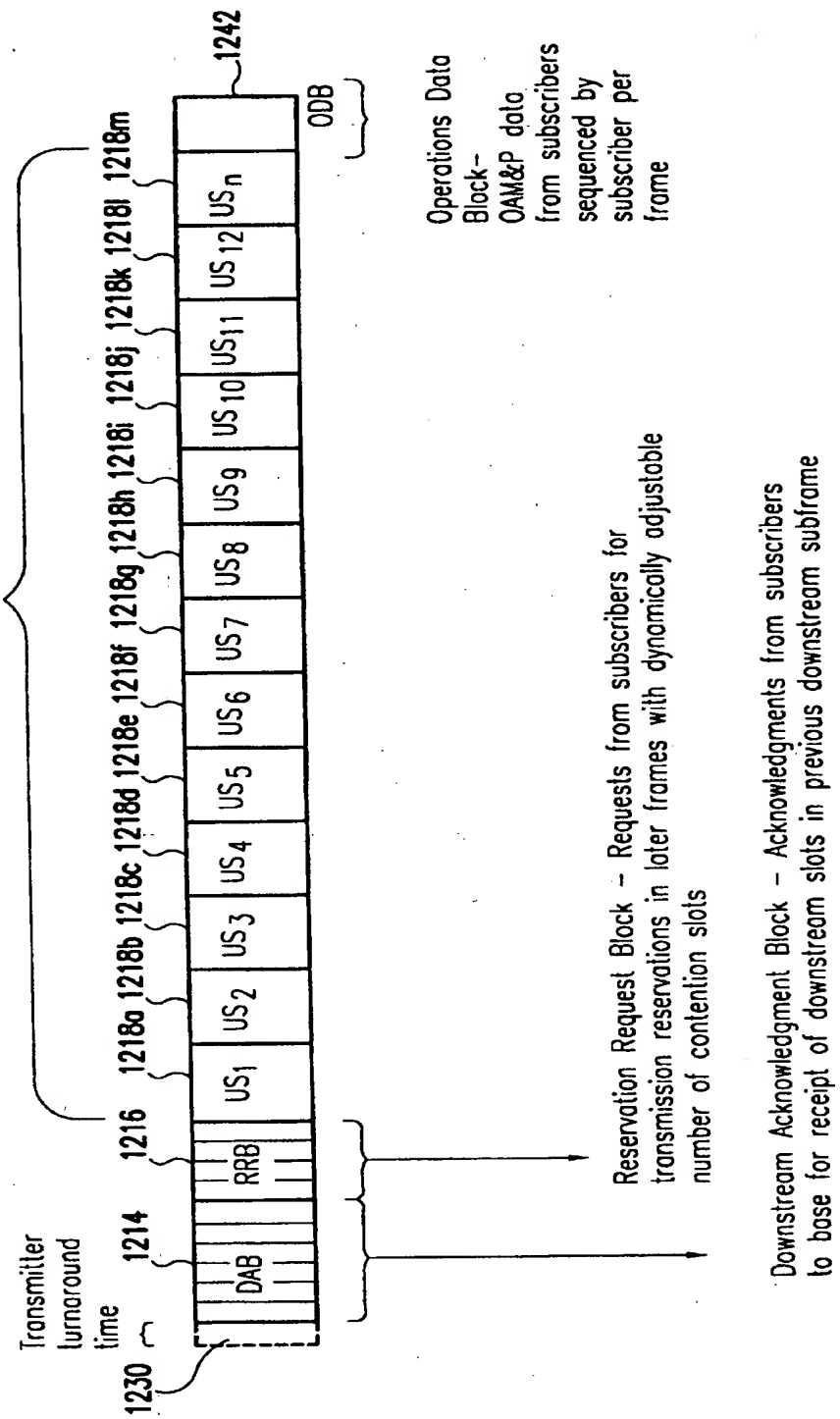

1204
Upstream slot transmissions
(variable number per frame up to 16)
1242
ODB
Operations Data Block–
OAM&P data from subscribers sequenced by subscriber per frame
Transmitter turnaround time
1230
1214
DAB
1216
RRB
1218a
US1
1218b
US2
1218c
US3
1218d
US4
1218e
US5
1218f
US6
1218g
US7
1218h
US8
1218i
US9
1218j
US10
1218k
US11
1218l
US12
1218m
USn
Reservation Request Block – Requests from subscribers for transmission reservations in later frames with dynamically adjustable number of contention slots
Downstream Acknowledgment Block – Acknowledgments from subscribers to base for receipt of downstream slots in previous downstream subframe

FIG. 12I

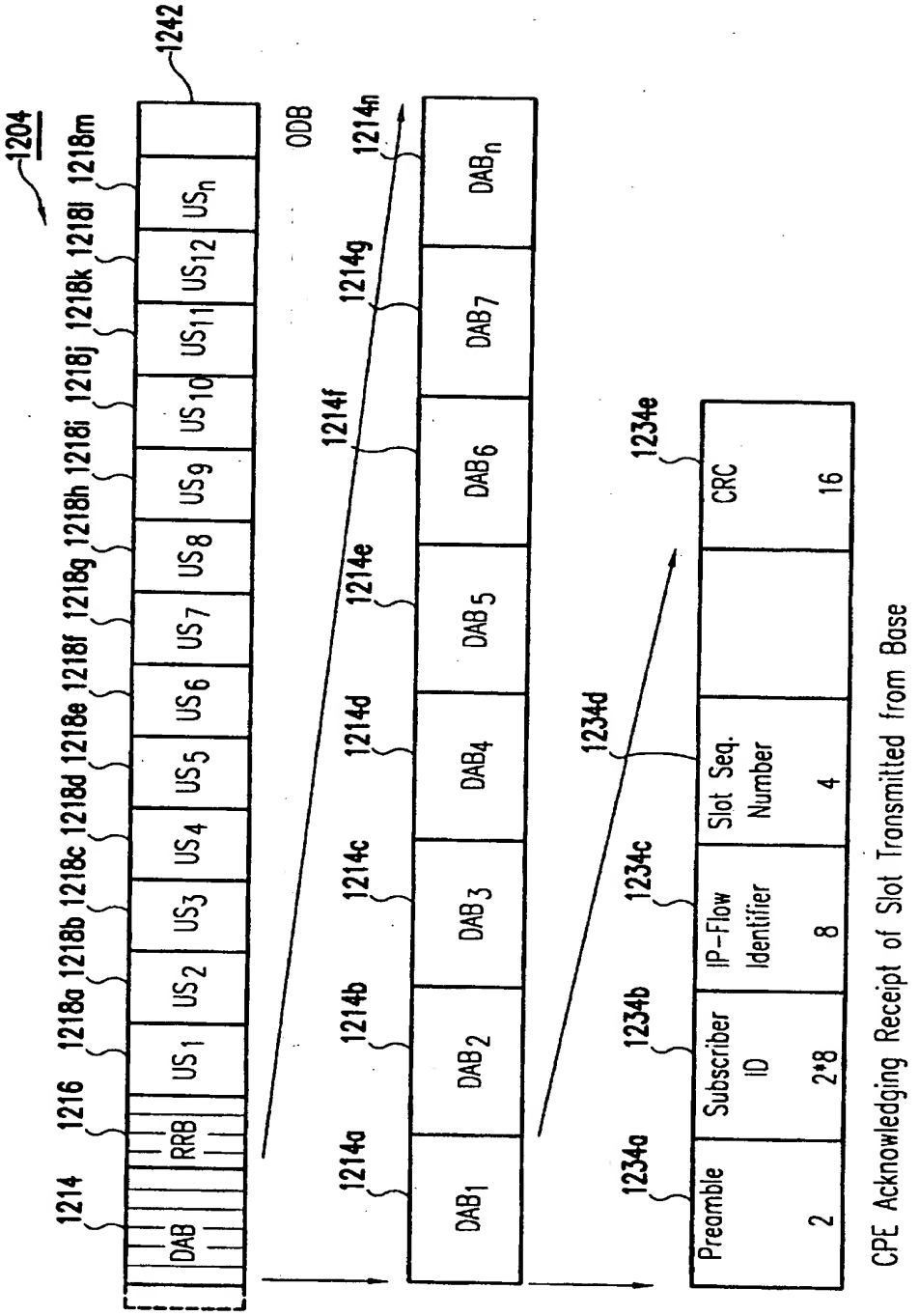
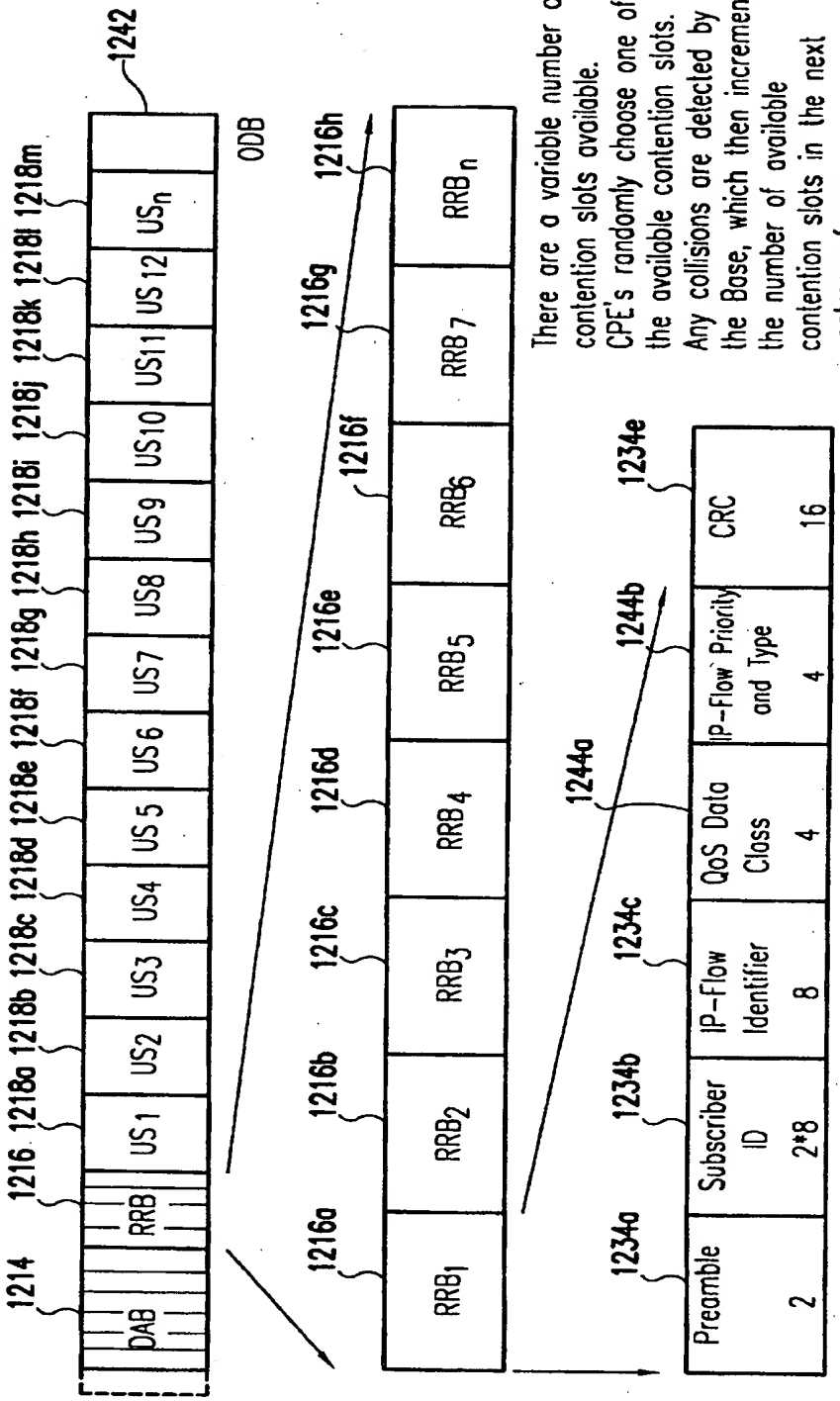


FIG. 12J

CPE Acknowledging Receipt of Slot Transmitted from Base



CPE Requesting a Reservation for Upstream Transmission of Slot

FIG. 12K

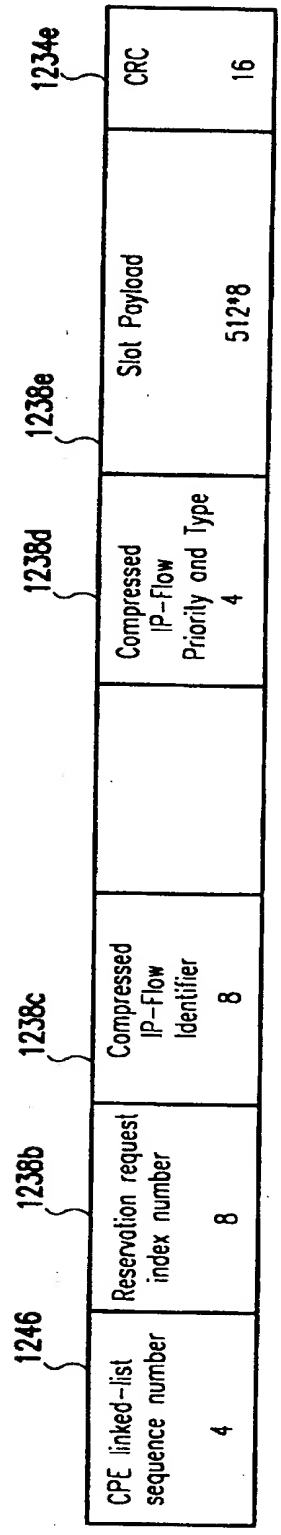

1246
CPE linked-list sequence number
4
1238b
Reservation request index number
8
1238c
Compressed IP-Flow Identifier
8
1238d
Compressed IP-Flow Priority and Type
4
1238e
Slot Payload
512*8
1234e
CRC
16

FIG. 12L

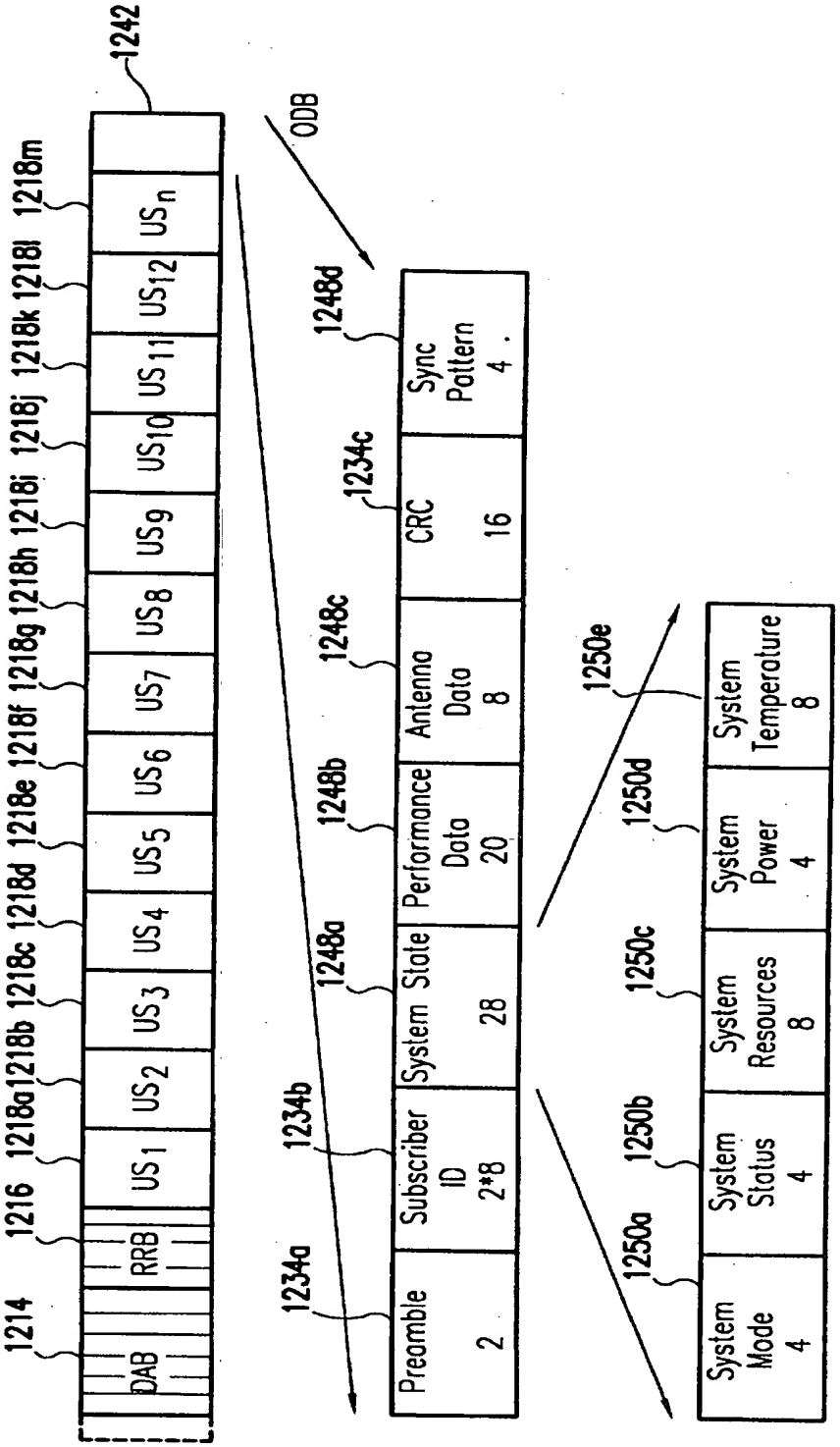

1242
1218m
1218l
1218k
1218j
1218i
1218h
1218g
1218f
1218e
1218d
1218c
1218b
1218a
1216
1214
DAB
RRB
US1
US2
US3
US4
US5
US6
US7
US8
US9
US10
US11
US12
USn
ODB
1248d
1248c
1248b
1248a
1234c
1234b
1234a
Sync Pattern 4
CRC 16
Antenna Data 8
Performance Data 20
System State 28
Subscriber ID 2*8
Preamble 2
1250e
1250d
1250c
1250b
1250a
System Temperature 8
System Power 4
System Resources 8
System Status 4
System Mode 4

FIG. 12M

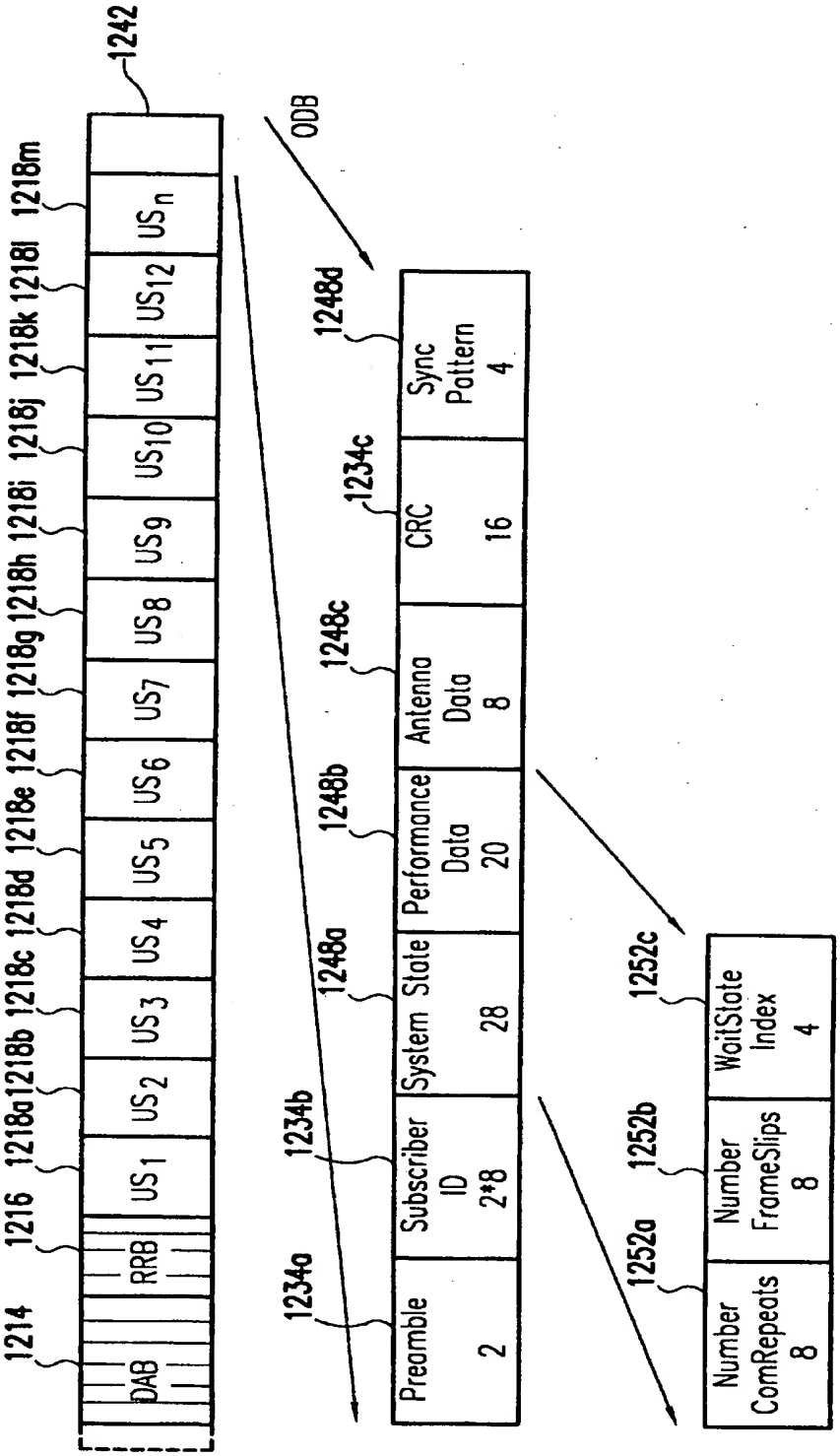

1242
1218m
1218l
1218k
1218j
1218i
1218h
1218g
1218f
1218e
1218d
1218c
1218b
1218a
1216
1214
DAB
RRB
US1
US2
US3
US4
US5
US6
US7
US8
US9
US10
US11
US12
USn
ODB
1248d
1234c
1248c
1248b
1234b
1248a
1234a
1252c
1252b
1252a
Sync Pattern 4
CRC 16
Antenna Data 8
Performance Data 20
System State 28
Subscriber ID 2*8
Preamble 2
WaitState Index 4
Number FrameSlips 8
Number ComRepeats 8

FIG.12N

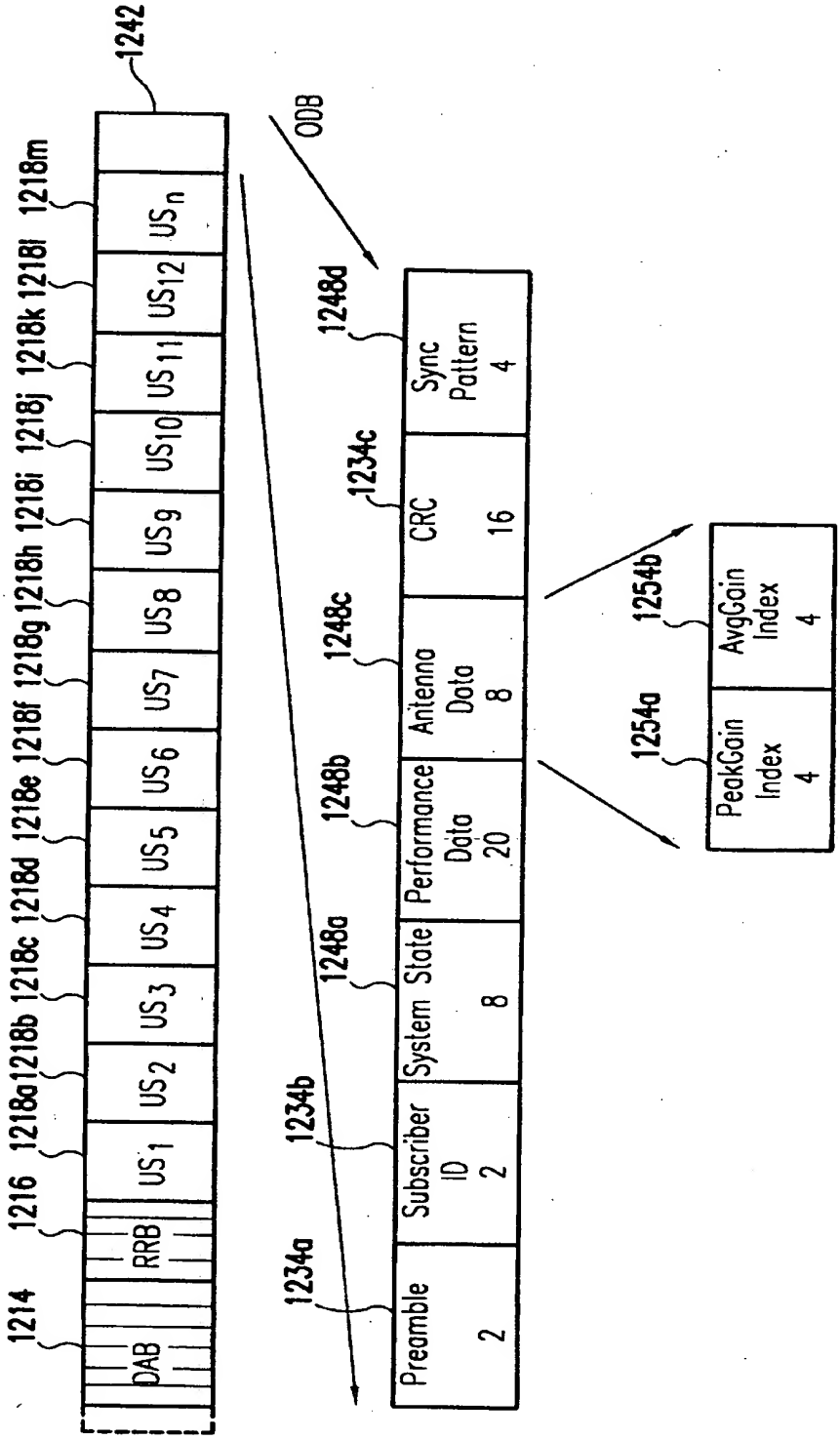

1242
ODB
1214
DAB
1216
RRB
1218a
US1
1218b
US2
1218c
US3
1218d
US4
1218e
US5
1218f
US6
1218g
US7
1218h
US8
1218i
US9
1218j
US10
1218k
US11
1218l
US12
1218m
USn
1234a
Preamble
2
1234b
Subscriber ID
2
1248a
System State
8
1248b
Performance Data
20
1248c
Antenna Data
8
1234c
CRC
16
1248d
Sync Pattern
4
1254a
PeakGain Index
4
1254b
AvgGain Index
4

FIG.120

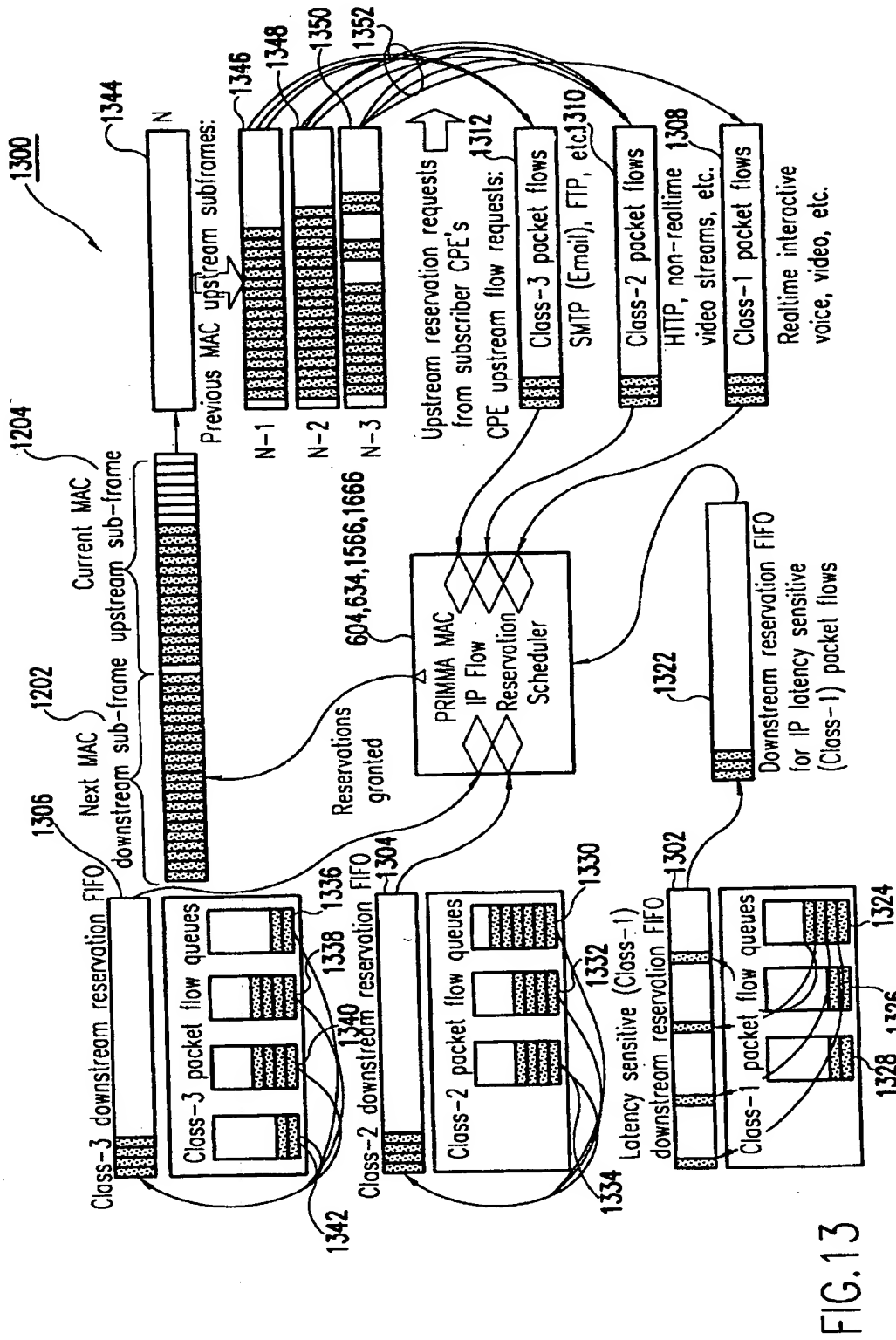

1300
1344
N
1346
1348
1350
1352
Previous MAC upstream subframes:
N-1
N-2
N-3
1204
Current MAC
downstream sub-frame upstream sub-frame
1202
Next MAC
downstream sub-frame
1306
Class-3 downstream reservation FIFO
Class-3 packet flow queues
1338
1336
1340
1342
1304
Class-2 downstream reservation FIFO
Class-2 packet flow queues
1330
1332
1334
1302
Latency sensitive (Class-1) downstream reservation FIFO
Class-1 packet flow queues
1324
1326
1328
Reservations granted
604,634,1566,1666
PRIMMA MAC IP Flow Reservation Scheduler
Upstream reservation requests from subscriber CPE's
CPE upstream flow requests:
1312
Class-3 packet flows
SMTP (Email), FTP, etc.
1310
Class-2 packet flows
HTTP, non-realtime video streams, etc.
1308
Class-1 packet flows
Realtime interactive voice, video, etc.
1322
Downstream reservation FIFO for IP latency sensitive (Class-1) packet flows

FIG. 13

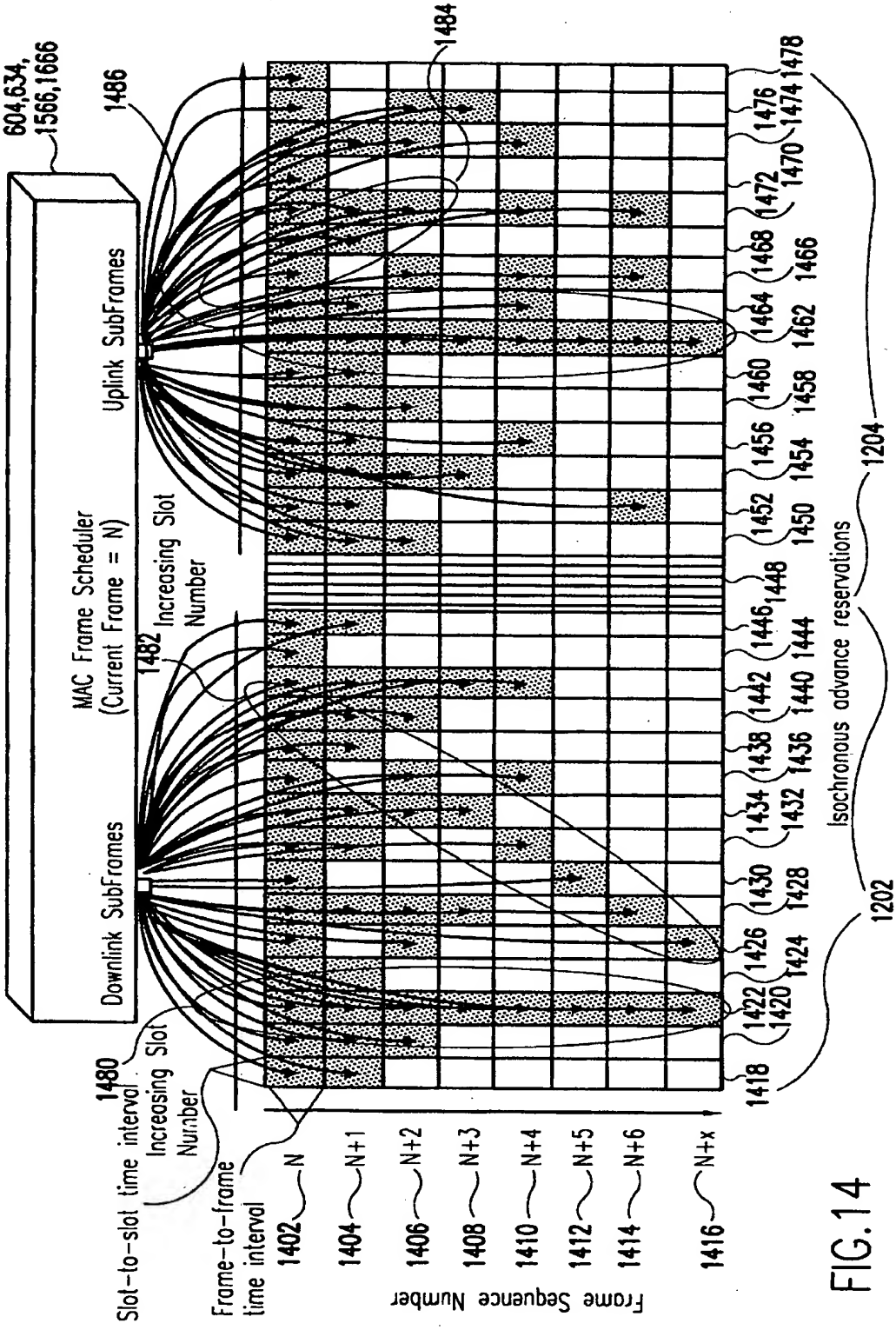

604,634,
1566,1666
1486
1484
MAC Frame Scheduler
(Current Frame = N)
Uplink SubFrames
Downlink SubFrames
Increasing Slot
Number
1482
1480
Slot-to-slot time interval
Increasing Slot
Number
Frame-to-frame
time interval
1402 N
1404 N+1
1406 N+2
1408 N+3
1410 N+4
1412 N+5
1414 N+6
1416 N+x
Frame Sequence Number
1418 1420 1422 1424 1426 1428 1430 1432 1434 1436 1438 1440 1442 1444 1446 1448 1450 1452 1454 1456 1458 1460 1462 1464 1466 1468 1470 1472 1474 1476 1478
1202
Isochronous advance reservations
1204

FIG. 14

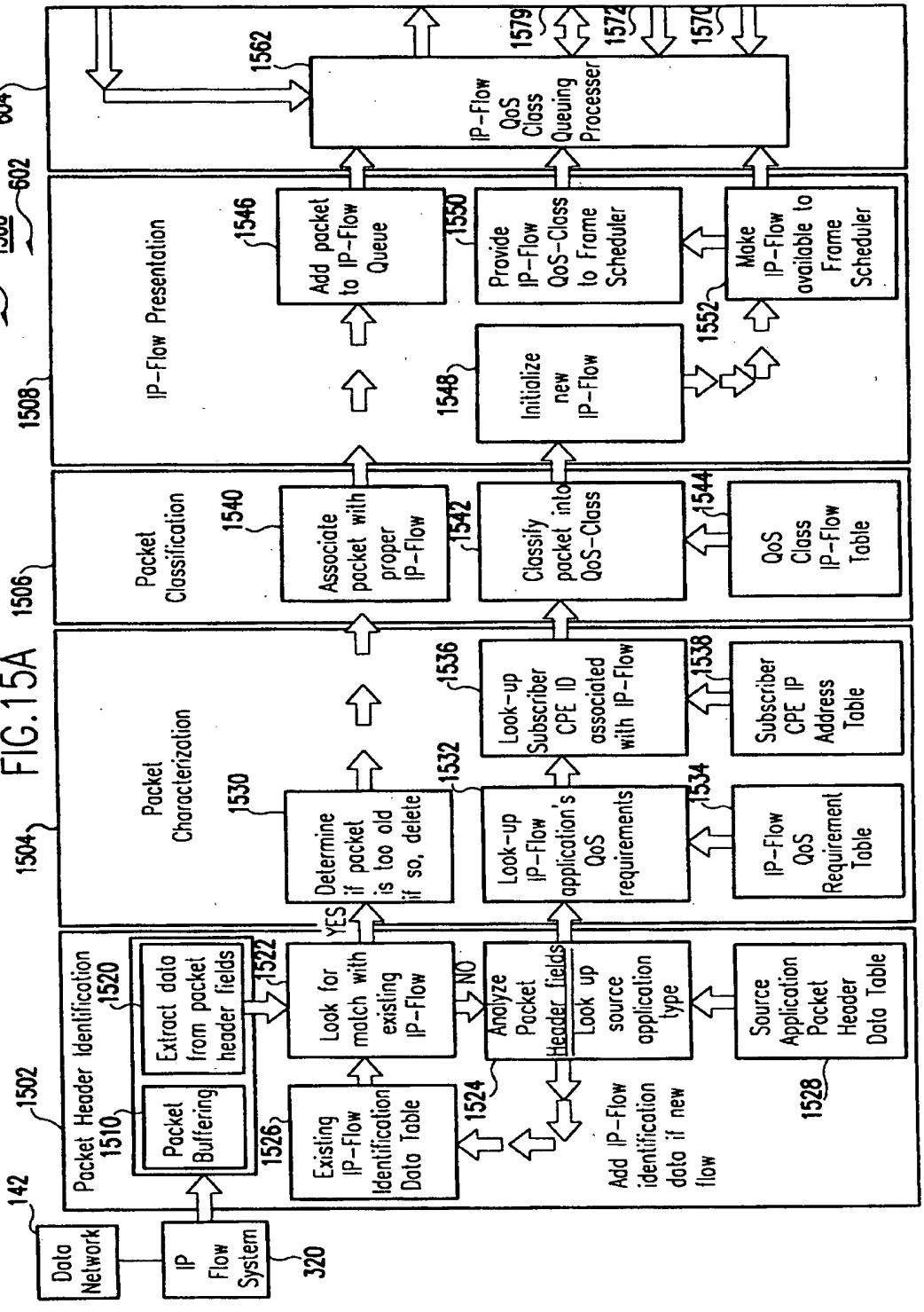

142
Data Network
IP Flow System
320
1502
Packet Header Identification
1520
Extract data from packet header fields
1522
Packet Buffering
1510
1526
Existing IP-Flow Identification Data Table
Look for match with existing IP-Flow
YES
NO
1524
Analyze Packet Header fields
Look up source application type
Add IP-Flow identification data if new flow
1528
Source Application Packet Header Data Table
1504
Packet Characterization
1530
Determine if packet is too old if so, delete
1532
Look-up IP-Flow application's QoS requirements
1534
IP-Flow QoS Requirement Table
1536
Look-up Subscriber CPE ID associated with IP-Flow
1538
Subscriber CPE IP Address Table
1506
Packet Classification
1540
Associate packet with proper IP-Flow
1542
Classify packet into QoS-Class
1544
QoS Class IP-Flow Table
1508
IP-Flow Presentation
1546
Add packet to IP-Flow Queue
1548
Initialize new IP-Flow
1550
Provide IP-Flow QoS-Class to Frame Scheduler
1552
Make IP-Flow available to Frame Scheduler
1500
602
604
1562
IP-Flow QoS Class Queuing Processer
1579
1572
1570

FIG. 15A

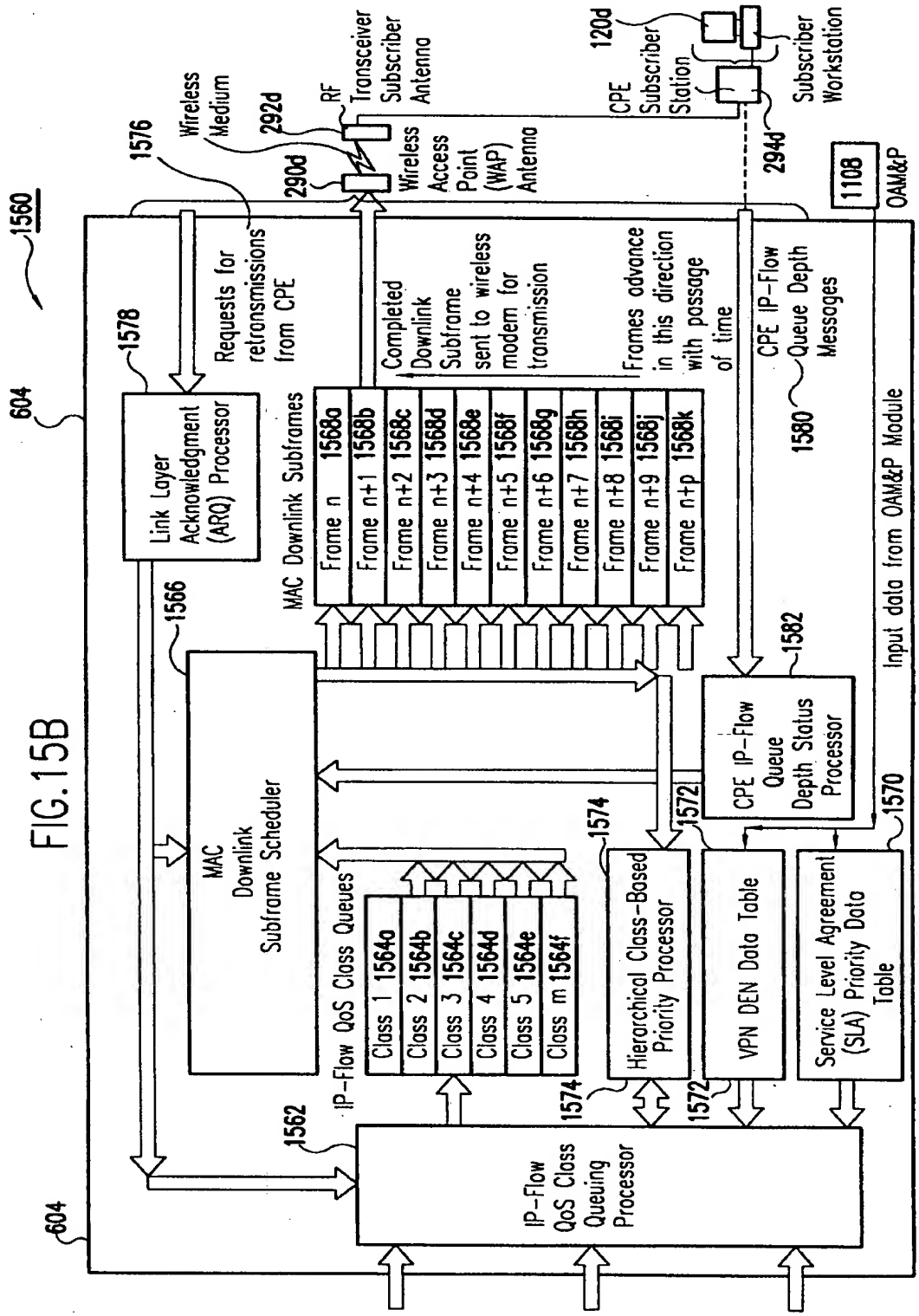

1560
604
1576
Wireless Medium
292d
RF Transceiver Subscriber Antenna
290d
Wireless Access Point (WAP) Antenna
120d
CPE Subscriber Station
Subscriber Workstation
294d
1108
OAM&P
1578
Link Layer Acknowledgment (ARQ) Processor
Requests for retransmissions from CPE
Completed Downlink Subframe sent to wireless modem for transmission
Frames advance in this direction with passage of time
CPE IP-Flow Queue Depth Messages
1580
MAC Downlink Subframes
Frame n 1568a
Frame n+1 1568b
Frame n+2 1568c
Frame n+3 1568d
Frame n+4 1568e
Frame n+5 1568f
Frame n+6 1568g
Frame n+7 1568h
Frame n+8 1568i
Frame n+9 1568j
Frame n+p 1568k
1566
1582
MAC Downlink Subframe Scheduler
CPE IP-Flow Queue Depth Status Processor
Input data from OAM&P Module
1574
1572
1570
IP-Flow QoS Class Queues
Class 1 1564a
Class 2 1564b
Class 3 1564c
Class 4 1564d
Class 5 1564e
Class m 1564f
Hierarchical Class-Based Priority Processor
VPN DEN Data Table
Service Level Agreement (SLA) Priority Data Table
1562
IP-Flow QoS Class Queuing Processor
604

FIG.15B

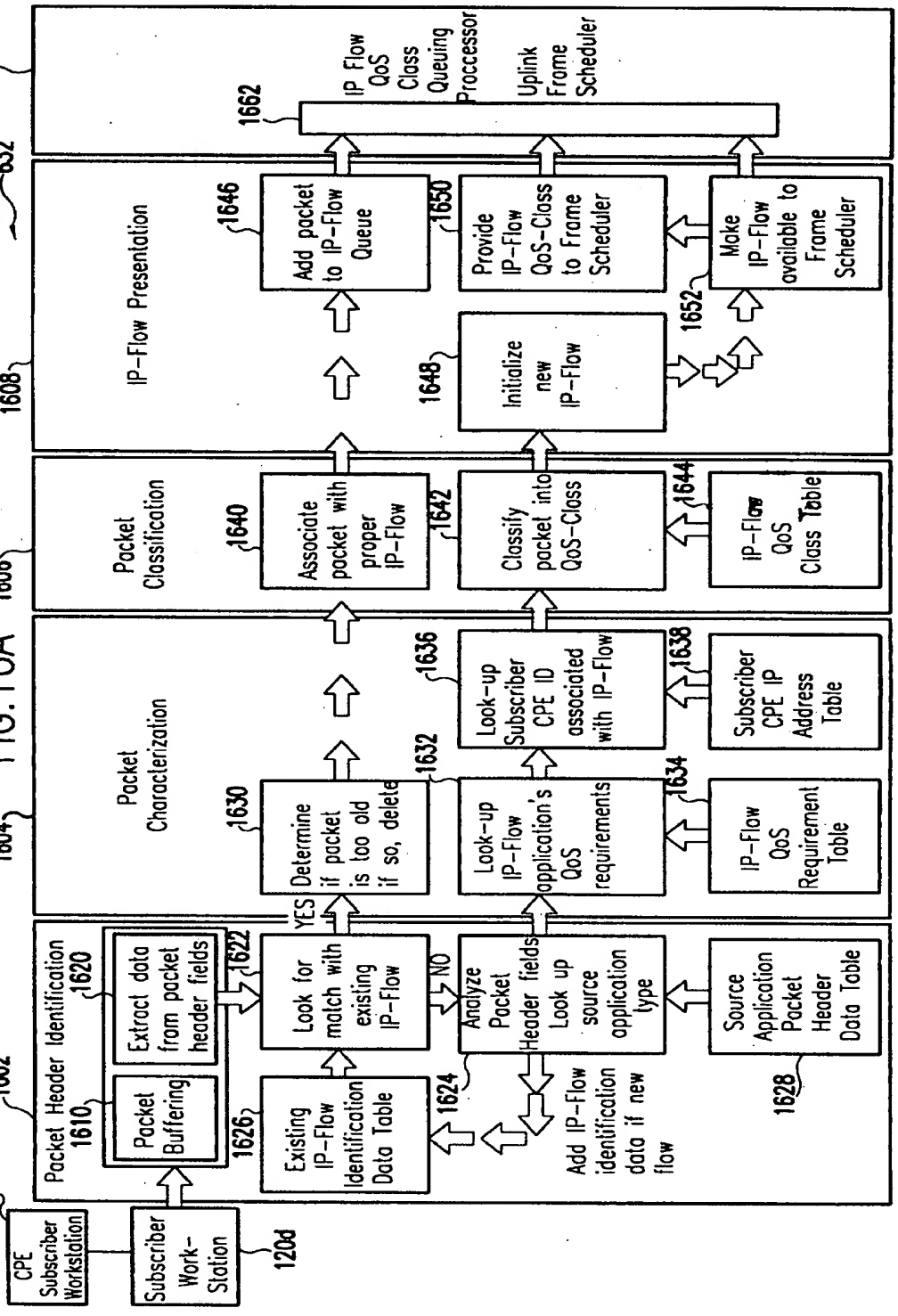

CPE Subscriber Workstation
Subscriber Work-Station
120d
294d
Packet Header Identification
1602
Packet Buffering
1610
Extract data from packet header fields
1620
1622
Existing IP-Flow Identification Data Table
1626
Look for match with existing IP-Flow
YES
NO
Analyze Packet Header fields
Look up source application type
1624
Add IP-Flow identification data if new flow
Source Application Packet Header Data Table
1628
Packet Characterization
1604
Determine if packet is too old if so, delete
1630
Look-up IP-Flow application's QoS requirements
1632
IP-Flow QoS Requirement Table
1634
Look-up Subscriber CPE ID associated with IP-Flow
1636
Subscriber CPE IP Address Table
1638
Packet Classification
1606
Associate packet with proper IP-Flow
1640
Classify packet into QoS-Class
1642
IP-Flow QoS Class Table
1644
IP-Flow Presentation
1608
Add packet to IP-Flow Queue
1646
Initialize new IP-Flow
1648
Provide IP-Flow QoS-Class to Frame Scheduler
1650
Make IP-Flow available to Frame Scheduler
1652
1600
632
634
IP Flow QoS Class Queuing Proccessor
1662
Uplink Frame Scheduler

FIG. 16A

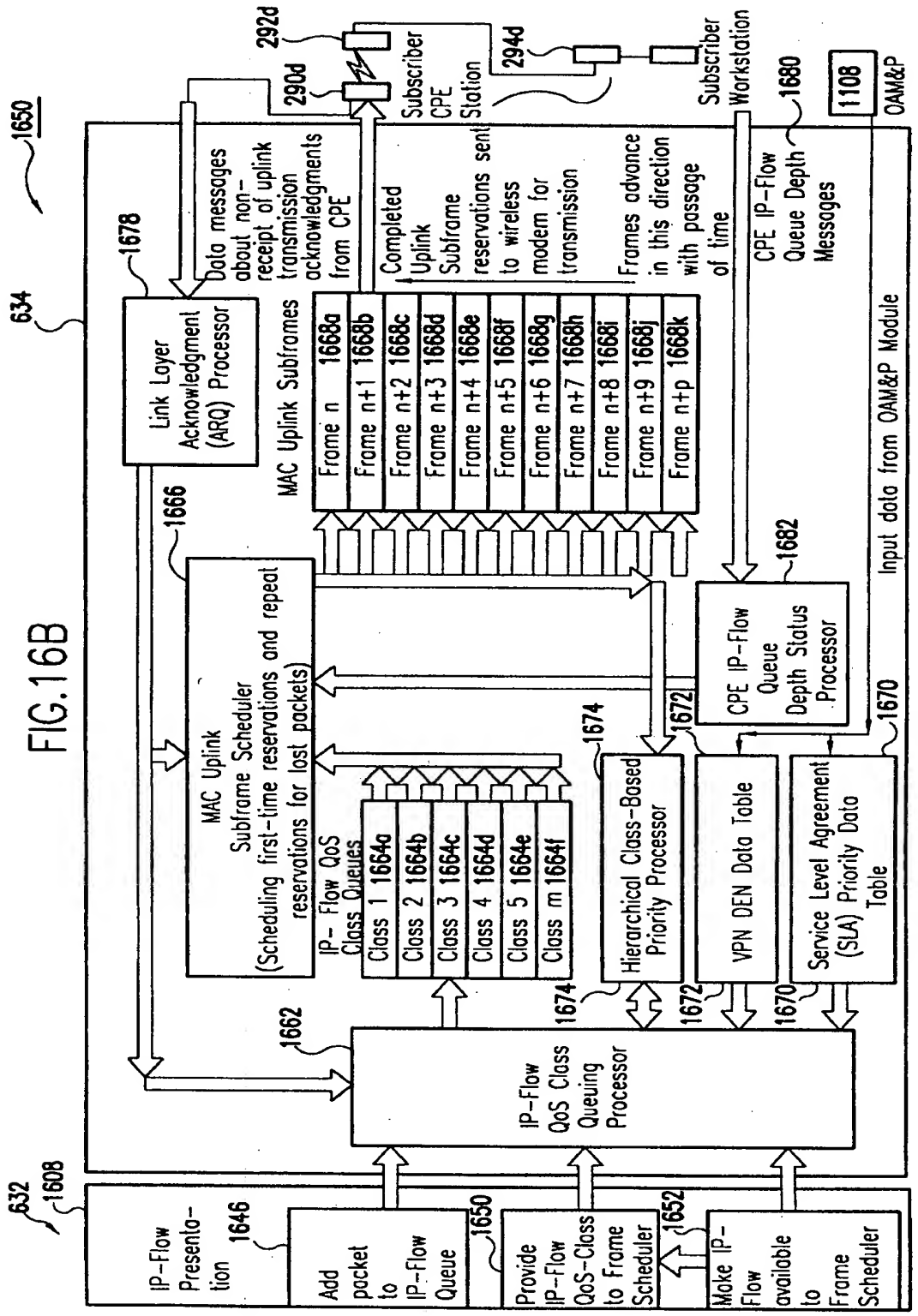

1650
634
632
1608
1678
1666
1662
1674
1672
1670
1682
1680
1108
1646
1650
1652
292d
290d
294d
Subscriber CPE Station
Subscriber Workstation
OAM&P
Data messages about non-receipt of uplink transmission acknowledgments from CPE
Completed Uplink Subframe reservations sent to wireless modem for transmission
Frames advance in this direction with passage of time
CPE IP-Flow Queue Depth Messages
Input data from OAM&P Module
Link Layer Acknowledgment (ARQ) Processor
MAC Uplink Subframes
Frame n 1668a
Frame n+1 1668b
Frame n+2 1668c
Frame n+3 1668d
Frame n+4 1668e
Frame n+5 1668f
Frame n+6 1668g
Frame n+7 1668h
Frame n+8 1668i
Frame n+9 1668j
Frame n+p 1668k
MAC Uplink Subframe Scheduler (Scheduling first-time reservations and repeat reservations for lost packets)
IP- Flow QoS Class Queues
Class 1 1664a
Class 2 1664b
Class 3 1664c
Class 4 1664d
Class 5 1664e
Class m 1664f
Hierarchical Class-Based Priority Processor
CPE IP-Flow Queue Depth Status Processor
VPN DEN Data Table
Service Level Agreement (SLA) Priority Data Table
IP-Flow QoS Class Queuing Processor
IP-Flow Presenta-tion
Add packet to IP-Flow Queue
Provide IP-Flow QoS-Class to Frame Scheduler
Make IP-Flow available to Frame Scheduler

FIG.16B

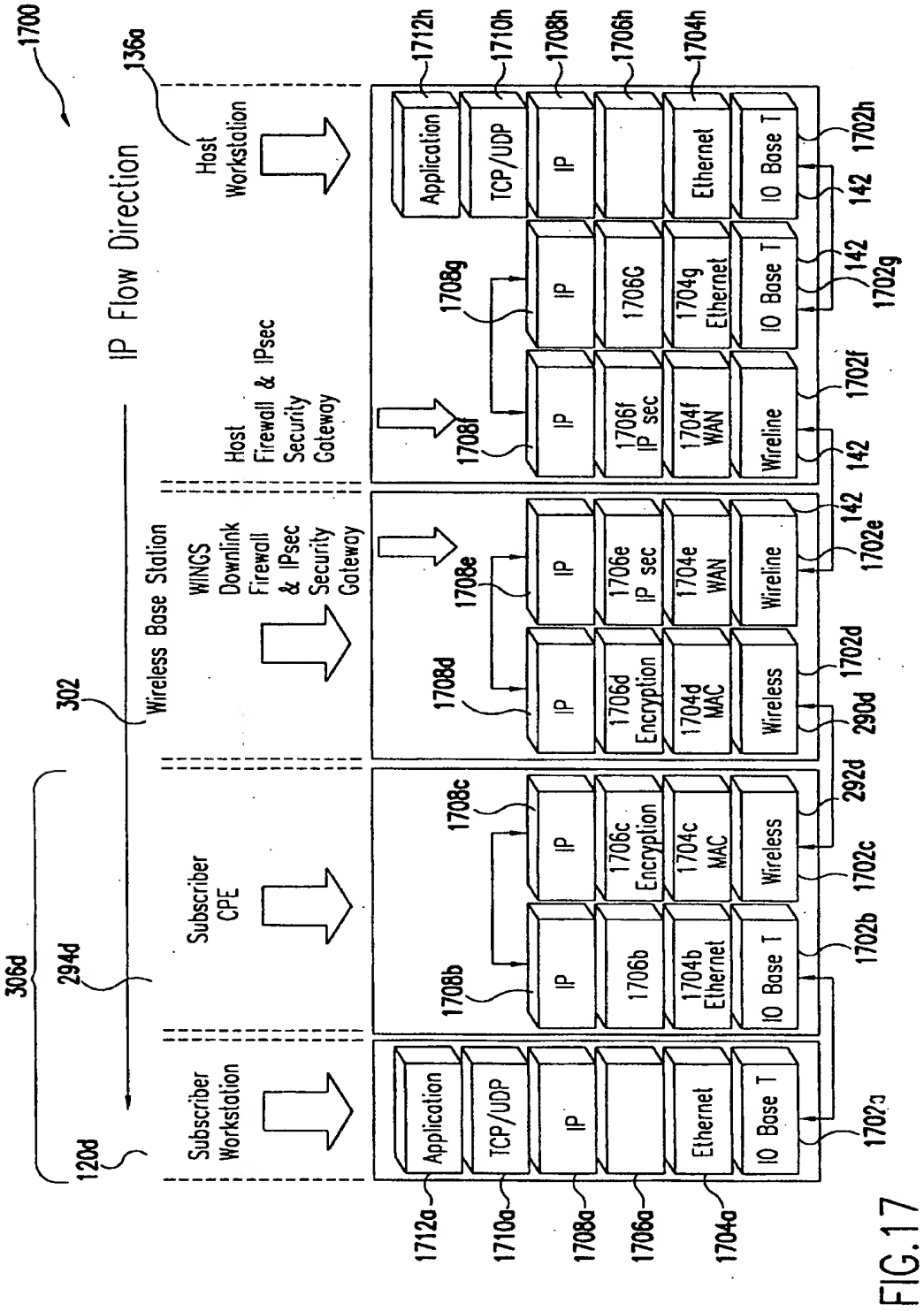

1700
IP Flow Direction
136a
Host Workstation
Host Firewall & IPsec Security Gateway
WINGS Downlink Firewall & IPsec Security Gateway
Subscriber CPE
Subscriber Workstation
Wireless Base Station
302
306d
294d
120d
Application
TCP/UDP
IP
Ethernet
IO Base T
1706f IP sec
1704f WAN
Wireline
1706G
1704g Ethernet
1706e IP sec
1704e WAN
1706d Encryption
1704d MAC
Wireless
1706c Encryption
1704c MAC
1706b
1704b Ethernet
1712h
1710h
1708h
1706h
1704h
1708g
1708f
1708e
1708d
1708c
1708b
1712a
1710a
1708a
1706a
1704a
1702h
1702g
1702f
1702e
1702d
1702c
1702b
1702a
142
290d
292d
294d

FIG. 17

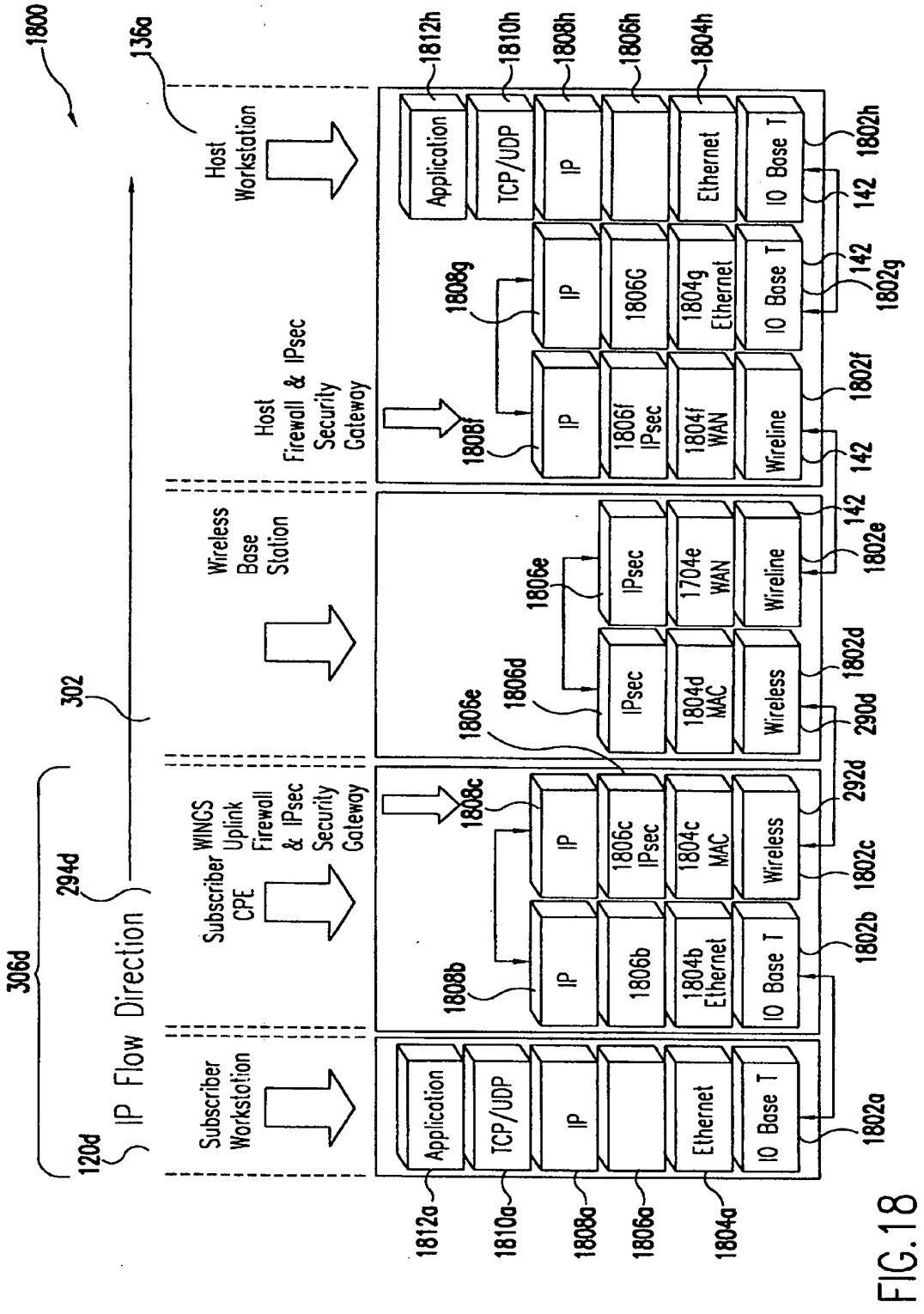

1800
136a
Host Workstation
Application
TCP/UDP
IP
Ethernet
10 Base T
1812h
1810h
1808h
1806h
1804h
1802h
142
1808g
1806G
1804g Ethernet
1802g
Host Firewall & IPsec Security Gateway
1808f
1806f IPsec
1804f WAN
Wireline
1802f
Wireless Base Station
1806e
IPsec
1704e WAN
1802e
1806d
1804d MAC
Wireless
290d
1802d
302
294d
306d
Subscriber CPE
WINGS Uplink Firewall & IPsec Security Gateway
1808c
1806c IPsec
1804c MAC
292d
1802c
IP Flow Direction
120d
Subscriber Workstation
1808b
1806b
1804b Ethernet
1802b
1812a
1810a
1808a
1806a
1804a
1802a

FIG. 18

IP-FLOW CLASSIFICATION IN A WIRELESS POINT TO MULTI-POINT (PTMP) TRANSMISSION SYSTEM

This application claims benefit of priority from U.S. Provisional Patent Application No. 60/092,452, filed Jul. 10, 1998.

CROSS-REFERENCE TO OTHER APPLICATIONS

The following applications of common assignee contain common disclosure:

U.S. patent application Ser. No. 09/349,477 entitled "Transmission Control Protocol/Internet Protocol (TCP/IP) Packet-Centric Wireless Point to Multi-Point (PtMP) Transmission System Architecture," filed Jul. 9, 1999,

U.S. patent application Ser. No. 09/349,480 entitled "Quality of Service (QoS)—Aware Wireless Point to Multi-Point (PtMP) Transmission System Architecture," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/350,126 entitled "Method for Providing Dynamic Bandwidth Allocation Based on IP-Flow Characteristics in a Wireless Point to Multi-Point (PtMP) Transmission System," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/350,118 entitled "Method for Providing for Quality of Service (QoS)—Based Handling of IP-Flows in a Wireless Point to Multi-Point Transmission System," filed Jul. 9, 1999,

U.S. patent application Ser. No. 09/347,356 entitled "IP-Flow Identification in a Wireless Point to Multi-Point Transmission System," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/350,150 entitled "IP-Flow Characterization in a Wireless Point to Multi-Point (PtMP) Transmission System," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/349,476 entitled "IP-Flow Prioritization in a Wireless Point to Multi-Point (PtMP) Transmission System," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/350,170 entitled "Method of Operation for Providing for Service Level Agreement (SLA) Based Prioritization in a Wireless Point to Multi-Point (PtMP) Transmission System," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/349,481 entitled "Method for Transmission Control Protocol (TCP) Rate Control With Link-Layer Acknowledgments in a Wireless Point to Multi-Point (PtMP) Transmission System," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/350,159 entitled "Transmission Control Protocol/Internet Protocol (TCP/IP)—Centric QoS Aware Media Access Control (MAC) Layer in a Wireless Point to Multi-Point (PtMP) Transmission System," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/347,857 entitled "Use of Priority-Based Scheduling for the Optimization of Latency and Jitter Sensitive IP Flows in a Wireless Point to Multi-Point Transmission System," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/349,475 entitled "Time Division Multiple Access/Time Division Duplex (TDMA/TDD) Access Method for a Wireless Point to Multi-Point Transmission System," filed Jul. 9, 1999.

U.S. patent application entitled Ser. No. 09/349,483 "Reservation Based Prioritization Method for Wireless Transmission of Latency and Jitter Sensitive IP-Flows in a Wireless Point to Multi-Point Transmission System," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/349,479 entitled "Translation of Internet-Prioritized Internet Protocol (IP)—Flows into Wireless System Resource Allocations in a Wireless Point to Multi-Point (PtMP) Transmission System," filed Jul. 9, 1999.

U.S. patent application entitled Ser. No. 09/350,162 "Method of Operation for the Integration of Differentiated services (Diff-serv) Marked IP-Flows into a Quality of Service (QoS) Priorities in a Wireless Point to Multi-Point (PtMP) Transmission System," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/349,975 entitled "Method for the Recognition and Operation of Virtual Private Networks (VPNs) over a Wireless Point to Multi-Point (PtMP) Transmission System," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/350,173 entitled "Time Division Multiple Access/Time Division Duplex (TDMA/TDD) Transmission Media Access Control (MAC) Air Frame," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/349,482 entitled "Application—Aware, Quality of Service (QoS) Sensitive, Media Access Control (MAC) Layer," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/349,478 entitled "Transmission Control Protocol/Internet Protocol (TCP/IP) Packet-Centric Wireless Point to Point (PtP) Transmission System Architecture," filed Jul. 9, 1999.

U.S. patent application Ser. No. 09/349,474 entitled "Transmission Control Protocol/Internet Protocol (TCP/IP) Packet-Centric Cable Point to Multi-Point (PtMP) Transmission System Architecture," filed Jul. 9, 1999.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to telecommunications and, more particularly, to a system and method for implementing a QoS aware wireless point-to-multi-point transmission system.

2. Related Art

Telecommunication networks such as voice, data and video networks have conventionally been customized for the type of traffic each is to transport. For example, voice traffic is very latency sensitive but quality is less important, so voice networks are designed to transport voice traffic with limited latency. Traditional data traffic, such as, e.g., a spreadsheet, on the other hand is not latency sensitive, but error-free delivery is required. Conventional telecommunications networks use circuit switching to achieve acceptable end user quality of service (QoS). With the advent of new packet switching high bandwidth data networks, different types of traffic can be transported over a data network. Specifically, convergence of separate voice, data and video networks into a single broadband telecommunications network is enabled. To ensure end user satisfaction, a system is desired that provides QoS for various types of traffic to be transported.

Wireless networks present particular challenges over their wireline counterparts in delivering QoS. For example, wireless networks traditionally exhibit high bit error rates (BER) due to a number of reasons. Conventional wireless networks also implement circuit switched connections to provide reliable communications channels. However the use of circuit switched connections allocates bandwidth between communicating nodes whether or not traffic is constantly being transferred between the nodes. Therefore, circuit switched connections use communications bandwidth rather inefficiently.

Packet switching makes more efficient use of available bandwidth than does traditional circuit switching. Packet

switching breaks up traffic into so-called "packets" which can then be transported from a source node to a destination for reassembly. Thus a particular portion of bandwidth can be shared by many sources and destinations yielding more efficient use of bandwidth.

A wireless broadband access telecommunications system is desired which can provide a QoS capability that is comparable to that delivered by wireline broadband access devices. Conventionally, one of the barriers to the deployment of wireless broadband access systems has been the absence of acceptable QoS characteristics, while at the same time delivering bandwidth sufficient to qualify as broadband. Delivery of raw bandwidth over wireless media without acceptable QoS would not benefit end users. Likewise, the delivery of a high level of QoS at the cost of sufficient bandwidth would also not benefit endusers.

Conventional efforts to provide wireless broadband access systems have not granted sufficient priority to QoS as a guiding principle in architecting the wireless systems, resulting in sub-optimal designs. With the rapid emergence of the Internet, the packet switching paradigm, and transmission control protocol/internet protocol (TCP/IP) as a universal data protocol, it has become clear that a new wireless system design has become necessary.

What is needed then is an IP-centric wireless broadband access system with true QoS capabilities.

SUMMARY OF THE INVENTION

The present invention is directed to an IP flow classification system used in a wireless telecommunications system. More specifically, the IP flow classification system groups IP flows in a packet-centric wireless point to multipoint telecommunications system.

The classification system includes: a wireless base station coupled to a first data network; one or more host workstations coupled to the first data network; one or more subscriber customer premise equipment (CPE) stations in wireless communication with the wireless base station over a shared bandwidth using a packet-centric protocol; and one or more subscriber workstations coupled to each of the subscriber CPE stations over a second network; a resource allocation device optimizes end-user quality of service (QoS) and allocates shared bandwidth among the subscriber CPE stations; an analyzing and scheduling device analyzes and schedules internet protocol (IP) flow over the shared wireless bandwidth. The analyzing device includes the above IP flow classifier that classifies the IP flow.

In one embodiment, the classifier includes a means for associating a packet of an existing IP flow with the IP flow. The classifier can include a QoS grouping device that groups a packet of a new IP flow into a QoS class grouping. The QoS grouping device can include a determining device that determines and takes into account QoS class groupings for the IP flow. The QoS grouping device can include an optional differentiated services (Diff Serv) device that takes into account an optional Diff Servs field priority marking for the IP flow. The QoS grouping device can also include an optional type of service (TOS) device that takes into account any optional type of service (TOS) field priority marking for said IP flow.

The cross-referenced applications are incorporated herein by reference in their entireties.

BRIEF DESCRIPTION OF THE FIGURES

The present invention will be described with reference to the accompanying figures, wherein:

FIG. 1A is a block diagram providing an overview of a standard telecommunications network providing local exchange carrier services within one or more local access and transport areas;

FIG. 1B depicts an exemplary network including workstations coupled to a data network;

FIG. 1C illustrates a conventional video network, such as for example a cable television (CATV) network;

FIG. 2A is a block diagram illustrating an overview of a standard telecommunications network providing both local exchange carrier and interexchange carrier services between subscribers located in different local access and transport areas;

FIG. 2B illustrates a signaling network in detail;

FIG. 2C illustrates an exemplary network carrying voice, data and video traffic over a data network;

FIG. 2D depicts a network including a point-to-multipoint wireless network coupled via a router to a data network;

FIG. 3A depicts an exemplary perspective diagram of a point-to-multipoint network;

FIG. 3B depicts a block diagram further illustrating a wireless point-to-multipoint network;

FIG. 4 depicts a wireless Internet protocol network access architecture of the present invention;

FIG. 5A depicts Internet protocol flows from a subscriber host to a wireless base station, and through a wireline connection to a destination host;

FIG. 5B illustrates a functional flow diagram including an example functional description of a transmission control protocol adjunct agent performing an outgoing transmission control protocol spoof function;

FIG. 5C illustrates a functional flow diagram including an exemplary functional description of a transmission control protocol adjunct agent performing an incoming transmission control protocol spoof function;

FIG. 6 illustrates a block diagram representing scheduling of mixed Internet protocol flows;

FIG. 7 illustrates packet header field information which can be used to identify Internet protocol flows and the quality of service requirements of the Internet protocol flows;

FIG. 8A is a block diagram summarizing an exemplary downlink analysis, prioritization and scheduling function;

FIG. 8B is a block diagram summarizing an exemplary uplink analysis prioritization and scheduling function;

FIG. 9 illustrates how a downlink flow scheduler can take into account a service level agreement in prioritizing a frame slot and scheduling resource allocation;

FIG. 10 depicts an embodiment of an inventive media access control hardware architecture;

FIG. 11 is an exemplary software organization for a packet-centric wireless point to multi-point telecommunications system;

FIG. 12A illustrates an exemplary time division multiple access media access control air frame;

FIG. 12B illustrates an exemplary structure for a time division multiple access/time division duplex air frame;

FIG. 12C illustrates an exemplary downstream transmission subframe;

FIG. 12D illustrates an exemplary upstream acknowledgment block field of a downstream transmission subframe;

FIG. 12E illustrates an exemplary acknowledgment request block field of a downstream transmission subframe;

FIG. 12F illustrates an exemplary frame descriptor block field of a downstream transmission subframe;

FIG. 12G illustrates an exemplary downstream media access control payload data unit of a downstream transmission subframe;

FIG. 12H illustrates an exemplary command and control block of a downstream transmission subframe;

FIG. 12I illustrates an exemplary upstream transmission subframe;

FIG. 12J illustrates an exemplary downstream acknowledgment block of an upstream transmission subframe;

FIG. 12K illustrates an exemplary reservation request block of an upstream transmission subframe **1204**;

FIG. 12L illustrates an exemplary media access control payload data unit of an upstream transmission subframe;

FIGS. 12M, 12N and 12O illustrate an exemplary operations data block of an upstream transmission subframe;

FIG. 13 illustrates how an exemplary flow scheduler for the present invention functions;

FIG. 14 is an exemplary two-dimensional block diagram of an advanced reservation algorithm;

FIG. 15A is an exemplary logical flow diagram for a downlink flow analyzer;

FIG. 15B is an exemplary logical flow diagram for a downlink flow scheduler;

FIG. 16A is an exemplary logical flow diagram for an uplink flow analyzer;

FIG. 16B is an exemplary logical flow diagram for an uplink flow scheduler;

FIG. 17 illustrates Internet protocol flow in a downlink direction, including Internet protocol security encryption; and

FIG. 18 illustrates an uplink direction of Internet protocol security support.

In the figures, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. The figure in which an element first appears is indicated by the leftmost digit(s) in the reference number.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

I. An Example Environment

The present invention is described in terms of an example environment. The example environment uses a fixed wireless point-to-multi-point (PtMP) connection to transmit packetized data information including for example, IP telephony, video, data, received from a telecommunications carrier. As used herein, a telecommunications carrier can include US domestic entities (see Definitions below at section II) such as, e.g., ILECs, CLECs, IXCs, NGTs and Enhanced Service Providers (ESPs), as well as global entities such as PTTs and NEs, recognized by those skilled in the art. In addition, as used herein a telecommunications system includes domestic systems used by entities such as, e.g., ILECs, CLECs, IXCs and Enhanced Service Providers (ESPs), as well as global systems recognized by those skilled in the art.

In the preferred embodiment, the traffic arrives from a wide area network (WAN) connection.

Data traffic is received from a data network through a network router and can be demodulated from internet protocol (IP) format to, for example, the point-to-point protocol (PPP). Network routers can include, for example, a general purpose computer, such as the SUN workstation running routing software or a dedicated routing device such as various models from CISCO of San Jose, Calif., ASCEND of Alameda, Calif., NETOPIA of Alameda, Calif., or 3COM of Santa Clara, Calif.

In the alternative, a virtual private networking protocol, such as the point-to-point tunneling protocol (PPTP), can be used to create a "tunnel" between a remote user and a corporate data network. A tunnel permits a network administrator to extend a virtual private network from a server (e.g., a Windows NT server) to a data network (e.g., the Internet).

Although the invention is described in terms of this example environment, it is important to note that description in these terms is provided for purposes of illustration only. It is not intended that the invention be limited to this example environment or to the precise inter-operations between the above-noted devices. In fact, after reading the following description, it will become apparent to a person skilled in the relevant art how to implement the invention in alternative environments.

II. Definitions

Table 1 below defines common telecommunications terminology. These terms are used throughout the remainder of the description of the invention.

TABLE 1

Term	Definition
access tandem (AT)	An AT is a class ¾ switch used to switch calls between EOs in a LATA. An AT provides subscribers access to the IXCs, to provide long distance calling services. An access tandem is a network node. Other network nodes can include, for example, a CLEC, or other enhanced services provider (ESP), an international gateway or global point-of-presence (GPOP), or an intelligent peripheral (IP).
bearer (B) channels	Bearer (B) channels are digital channels used to carry both digital voice and digital data information. An ISDN bearer channel is 64,000 bits per second, which can carry PCM-digitized voice or data.
called party	The called party is the caller receiving a call sent over a network at the destination or termination end.
calling party	The calling party is the caller placing a call over any kind of network from the origination end.
central office (CO)	A CO is a facility that houses an EO homed. EOs are often called COs.
class 1 switch	A class 1 switching office, the Regional Center (RC), is the highest level of local and long distance switching, or "office of last resort" to complete a call.
class 3 switch	A class 3 switching office was a Primary Center (PC); an access tandem (AT) has class 3 functionality.
class 4 switch	A class 4 switching office was a Toll Center (TC) if operators were present or else a Toll Point (TP); an access tandem (AT) has class 4 functionality.
class 5 switch	A class 5 switching office is an end office (EO) or the lowest level of local and long distance switching, a local central office. The switch closest to the end subscriber.
competitive LEC (CLEC)	CLECs are telecommunications services providers of local services that can compete with ILECs. Interprise and Century 21 are examples. A CLEC may or may not handle IXC services as well.
competitive access providers (CAPS)	Teligent and Winstar are examples.
customer premises equipment (CPE)	CPE refers to devices residing on the premises of a customer and used to connect to a telephone network, including ordinary telephones, key telephone systems, PBXs, video conferencing devices and modems.

TABLE 1-continued

Term	Definition
digitized data (or digital data)	Digitized data refers to analog data that has been sampled into a binary representation (i.e., comprising sequences of 0's and 1's). Digitized data is less susceptible to noise and attenuation distortions because it is more easily regenerated to reconstruct the original signal.
egress end office	The egress EO is the node or destination EO with a direct connection to the called party, the termination point. The called party is "homed" to the egress EO.
egress	Egress refers to the connection from a called party or termination at the destination end of a network, to the serving wire center (SWC).
end office (EO)	An EO is a class 5 switch used to switch local calls within a LATA. Subscribers of the LEC are connected ("homed") to EOs, meaning that EOs are the last switches to which the subscribers are connected.
Enhanced Service Provider (ESP)	A network services provider.
equal access	1 + dialing as used in US domestic calling for access to any long distance carrier as required under the terms of the modified final judgment (MFJ) requiring divestiture of the Regional Bell Operating Companies (RBOCs) from their parent company, AT&T.
global point of presence (GPOP)	A GPOP refers to the location where international telecommunications facilities and domestic facilities interface, an international gateway POP.
incumbent LEC (ILEC)	ILECs are traditional LECs in the US, which are the Regional Bell Operating Companies (RBOCs). Bell South and US West are examples. ILEC can also stand for an independent LEC such as a GTE.
ingress end office	The ingress EO is the node or serving wire center (SVC) with a direct connection to the calling party, the origination point. The calling party is "homed" to the ingress EO.
ingress	Ingress refers to the connection from a calling party or origination.
integrated service digital network (ISDN) basic rate interface (BRI) line	An ISDN Basic Rate Interface (BRI) line provides 2 bearer B channels and 1 data D line (known as "2B+D" over one or two pairs) to a subscriber.
integrated services digital network (ISDN)	ISDN is a network that provides a standard for communications (voice, data and signaling), end-to-end digital transmission circuits, out-of-band signaling, and a features significant amount of bandwidth.
inter machine trunk (IMT)	An inter-machine trunk (IMT) is a circuit between two commonly-connected switches.
inter-exchange carrier (IXC)	IXCs are US domestic long distance telecommunications services providers. AT&T, MCI, Sprint, are examples.
internet protocol (IP)	IP is part of the TCP/IP protocols. It is used to recognize incoming messages, route outgoing messages, and keep track of Internet node addresses (using a number to specify a TCP/IP host on the Internet). IP corresponds to the network layer of OSI.
Internet service provider (ISP)	An ISP is a company that provides Internet access to subscribers.
ISDN primary rate interface (PRI)	An ISDN Primary Rate Interface (PRI) line provides the ISDN equivalent of a T1 circuit. The PRI delivered to a customer's premises can provide 23B+D (in North America) or 30B+D (in Europe) channels running at 1.544 megabits per second and 2.048 megabits per second, respectively.
local exchange carrier (LEC)	LECs are local telecommunications services providers. Bell Atlantic and US West are examples.
local access and transport area (LATA)	A LATA is a region in which a LEC offers services. There are over 160 LATAs of these local geographical areas within the United States.
local area network (LAN)	A LAN is a communications network providing connections between computers and peripheral devices (e.g., printers and modems) over a relatively short distance (e.g., within a building) under standardized control.
modified final judgment (MFJ)	Modified final judgment (MFJ) was the decision requiring divestiture of the Regional Bell Operating Companies (RBOCs) from their parent company, AT&T.
network node	A network node is a generic term for the resources in a telecommunications network, including switches, DACS, regenerators, etc. Network nodes essentially include all non-circuit (transport) devices. Other network nodes can include, for example, equipment of a CLEC, or other enhanced service provider (ESP), a point-of-presence (POP), an international gateway or global point-of-presence (GPOP).
new entrant (NE)	A new generation global telecommunications.
next generation telephone (NGT)	A new telecommunications services provider, especially IP telephony providers. Examples are Level 3 and Qwest.
packetized voice or voice over a backbone	One example of packetized voice is voice over internet protocol (VOIP). Voice over packet refers to the carrying of telephony or voice traffic over a data network, e.g. voice over frame, voice over ATM, voice over Internet Protocol (IP), over virtual private networks (VPNs), voice over a backbone, etc.
Pipe or dedicated communications facility	A pipe or dedicated communications facility connects an ISP to the internet.
point of presence (POP)	A POP refers to the location within a LATA where the IXC and LEC facilities interface.
point-to-point tunneling protocol (PPTP)	A virtual private networking protocol, point-to-point tunneling protocol (PPTP), can be used to create a "tunnel" between a remote user and a data network. A tunnel permits a network administrator to extend a virtual private network (VPN) from a server (e.g., a Windows NT server) to a data network (e.g., the Internet).
point-to-point (PPP) protocol	PPP is a protocol permitting a computer to establish a connection with the Internet using a modem. PPP supports high-quality graphical front ends, like Netscape.
postal telephone telegraph (PTT)	State regulated telephone companies, many of which are being deregulated. NTT is an example.
private branch exchange (PBX)	A PBX is a private switch located on the premises of a user. The user is typically a private company which desires to provide switching locally.
private line with a dial tone	A private line is a direct channel specifically dedicated to a customer's use between two specificed points. A private line with a dial tone can connect a PBX or an ISP's access concentrator to an end office (e.g. a channelized T1 or PRI). A private line can also be known as a leased line.
public switched telephone network (PSTN)	The PSTN is the worldwide switched voice network.
regional Bell operating companies (RBOCs)	RBOCs are the Bell operating companies providing LEC services after being divested from AT&T.
signaling system 7 (SS7)	SS7 is a type of common channel interoffice signaling (CCIS) used widely throughout the world. The SS7 network provides the signaling functions of indicating the arrival of calls, transmitting routing and destination signals, and monitoring line and circuit status.

TABLE 1-continued

Term	Definition
switching hierarchy or office classification	An office class is a functional ranking of a telephone central office switch depending on transmission requirements and hierarchical relationship to other switching centers. Prior to AT&T's divestiture of the RBOCs, an office classification was the number assigned to offices according to their hierarchical function in the U.S. public switched network (PSTN). The following class numbers are used: class 1 = Regional Center (RC), class 2 = Sectional Center (SC), class 3 = Primary Center (PC), class 4 = Toll Center (TC) if operators are present or else Toll Point (TP), class 5 = End Office (EO) a local central office. Any one center handles traffic from one to two or more centers lower in the hierarchy. Since divestiture and with more intelligent software in switching offices, these designations have become less firm. The class 5 switch was the closest to the end subscriber. Technology has distributed technology closer to the end user, diffusing traditional definitions of network switching hierarchies and the class of switches.
telecommunications carrier	A LEC, a CLEC, an IXC, an Enhanced Service Provider (ESP), an intelligent peripheral (IP), an international/global point-of-presence (GPOP), i.e., any provider of telecommunications services.
transmission control protocol (TCP)	TCP is an end-to-end protocol that operates at the transport and sessions layers of OSI, providing delivery of data bytes between processes running in host computers via separation and sequencing of IP packets.
transmission control protocol/internet protocol (TCP/IP)	TCP/IP is a protocol that provides communications between interconnected networks. The TCP/IP protocol is widely used on the Internet, which is a network comprising several large networks connected by high-speed connections.
trunk	A trunk connects an access tandem (AT) to an end office (EO).
wide area network (WAN)	A WAN is a data network that extends a LAN over the circuits of a telecommunications carrier. The carrier is typically a common carrier. A bridging switch or a router is used to connect the LAN to the WAN.

III. Introduction

A. Quality of Service (QOS) in a Wireless Environment

The concept of quality of service (QoS) is one of the most difficult and least understood topics in data networking. Although a common term in data networking, there are many different usages and definitions for QoS, leading to confusion regarding an exact meaning in precise or quantitative terms. Even further confusion is found when attempts are made to measure or specify numeric quantities sufficient to allow comparison of equipment or network performance with respect to QoS.

The confusion about QoS in general data networking is transferred and magnified when applied to wireless data communications. Wireless transmission has a higher inherent bit error rate (BER) than does wireline transmission. The addition of, e.g., a point-to-multipoint (PtMP) topology for multiple users sharing a wireless medium makes it desirable that QoS be defined in a manner that specifically addresses the multiple complicating factors in wireless data communications.

To provide a non-ambiguous definition of QoS that applies to wireless data communications, the nature of the problem that QoS is meant to solve is helpful. Many of the problems of data communications over wireless are unique and distinct from those of wireline data communications, while some are in fact shared. For wireless broadband access systems, the problems of quality delivery are somewhat more complex than for the wireline analog. Like its wireline counterpart, the problems encountered in wireless delivery of data include, e.g., slow peripheral access, data errors, "drop-outs," unnecessary retransmissions, traffic congestion, out-of-sequence data packets, latency, and jitter. In addition to these problems, wireless delivery adds problems including, e.g., high inherent bit error rates (BERs), limited bandwidth, user contention, radio interference, and TCP traffic rate management. A QoS-aware wireless system is desired to address all these problems.

There are a number of ways in which users or subscribers to a data network experience difficulties. One network difficulty is due to a lack of network availability. Depending on the access technology being used, this can include a "modem no-answer" condition, "network busy" condition, or a sudden unexpected "drop" of a network connection. These conditions would not be described as being consistent with high QoS. Once network connectivity is achieved, slow traffic caused by congestion, local access bottlenecks, and network failures can be experienced as slow web page loading, slow file transfers, or poor voice/video quality in streaming multimedia applications. Poor quality in streaming multimedia applications can instead result from high "jitter," or large and rapid variations in latency, leading to interruptions, distortion, or termination of session. Many different conditions can lead to actual data errors, which in some contexts can be catastrophic, such as in the file transfer of a spreadsheet. It is desirable that these problems of a data communications network be minimized or eliminated.

1. Quality

In data networking, quality usually implies the process of delivering data in a reliable and timely manner. What is reliable and timely is dependent on the nature of the traffic being addressed. These terms may include references to limitations in data loss, expectations of data accuracy, limitations of data latency variations (also known as jitter), and limitations of data retransmissions and limitations of data packet order inversions. Therefore, QoS is a complex concept, which can require a correspondingly complex mechanism to implement it.

QoS can be a relative term, finding different meanings for different users. A casual user doing occasional web browsing, but no file transfer protocol (FTP) file downloads or real time multimedia sessions may have different a different definition of QoS than a power user doing many FTP file downloads of large database or financial files, frequent H.323 video conferencing and IP telephony calls. Also, a user can pay a premium rate (i.e. a so-called service level agreement (SLA)) for high network availability, low latency, and low jitter, while another user can pay a low rate for occasional web surfing only, and on weekends only. Therefore, perhaps it is best to understand QoS as a continuum, defined by what network performance characteristic is most important to a particular user and the user's SLA. Maximizing the end-user experience is an essential component of providing wireless QoS.

2. Service

In data networking, a service can be defined as a type of connection from one end of a network to another. Formerly, this could have been further defined to be protocol specific, such as, e.g., IBM's systems network architecture (SNA), Novell's IPX, Digital's DECnet. However, it appears that TCP/IP (i.e. including user datagram protocol(UDP)) has evolved to become the overwhelming protocol of choice, and will continue to be in the foreseeable future. Therefore, service can be defined to be a particular type of TCP/IP

connection or transmission. Such service types might include, e.g., FTP file transfers, e-mail traffic, hypertext transfer protocol (HTTP) traffic, H.323 videoconferencing sessions. It is desirable that a QoS mechanism deal with these differing types of service, in addition to dealing with the different types of quality as discussed previously.

3. QOS as a Mechanism

QoS can be thought of as a mechanism to selectively allocate scarce networking, transmission and communications resources to differentiated classes of network traffic with appropriate levels of priority. Ideally, the nature of the data traffic, the demands of the users, the conditions of the network, and the characteristics of the traffic sources and destinations all modify how the QoS mechanism is operating at any given instant. Ultimately, however, it is desirable that the QoS mechanism operate in a manner that provides the user with optimal service, in whatever manner the user defines it.

a. Circuit-Switched QoS

In legacy networks created primarily for voice traffic by telephone companies, data transmission was accomplished with reference to a circuit-centric definition of QoS. In this definition, QoS implied the ability to carry asynchronous (i.e. transmission of data through start and stop sequences without the use of a common clock) as well as isochronous (i.e.consistent timed access of network bandwidth for time-sensitive voice and video) traffic. Circuit-switched QoS was accomplished by dedicating an end-to-end circuit for each connection or service, whether it was voice (see FIG. 1A) or data. The circuit-centric QoS mechanism was simply the provision of this circuit for exclusive use by the user. Of course, this approach dedicates the circuit, all transmission channels associated with the circuit, and the transport media itself to a single user for the entire duration of the session, regardless of whether data is actually being transmitted every instant of the session. It was generally believed that only in this manner could true QoS be achieved. Therefore, traditional designs for wireless broadband access systems (see FIG. 2A) also used this approach, dedicating a wireless radio channel to each particular data connection, regardless of the application or whether indeed any data was being transmitted at any given moment. This circuit-centric approach to QoS is fairly expensive, in terms of the cost of the equipment, and the utilization factors for the transmission media itself.

b. Asynchronous Transfer Mode (ATM) QoS

With ATM networking, telephone companies could continue to provide a circuit-centric QoS mechanism with the establishment of permanent virtual connections (PVCs) (i.e. a virtual path or channel connection (VPC or VCC) provisioned for indefinite use) and switched virtual connections (SVCs) (i.e. a logical connection between endpoints established by an ATM network on demand based upon signaling messages received from the end user or another network) in an analogous manner to the legacy voice circuit mechanism. However, several new concepts were needed, including admission policy, traffic shaping, and mechanisms such as, e.g., leaky-buckets, in order to handle traffic that was now categorized as variable bit rate (VBR), constant bit rate (CBR), and unspecified bit rate (UBR).

Virtual circuits were to be established for data transmission sessions, again regardless of the data application or whether data was being transmitted at any given moment. Although ATM provides QoS for broadband network traffic, the underlying assumptions of ATM design include the low BER characteristic of wireline networks, not the high BER of the wireless medium. Without a recognition of the characteristics of the traffic that is being carried by the ATM mechanism and the high inherent BER of wireless, true QoS can not be provided. ATM QoS mechanisms do not address the unique challenges associated with wireless communication.

c. Packet-Switched QoS

Packet-switching is revolutionizing data communications, so conventional circuit-switch and ATM networking concepts and their legacy QoS mechanisms are in need of update. With packet-switched data communications, one cannot dedicate a circuit to a particular data communications session. Indeed, a strength of packet-switching lies in route flexibility and parallelism of its corresponding physical network. Therefore, the QoS mechanism cannot work in the same manner as the legacy circuit-centric QoS mechanism did.

Simply providing "adequate" bandwidth is not a sufficient QoS mechanism for packet-switched networks, and certainly not for wireless broadband access systems. Although some IP-flows are "bandwidth-sensitive," other flows are latency- and/or jitter-sensitive. Real time or multimedia flows and applications cannot be guaranteed timely behavior by simply providing excessive bandwidth, even if it were not cost-prohibitive to do so. It is desirable that QoS mechanisms for an IP-centric wireless broadband access system recognize the detailed flow-by-flow requirements of the traffic, and allocate system and media resources necessary to deliver these flows in an optimal manner.

d. Summary—QoS Mechanisms

Ultimately, the end-user experience is the final arbiter of QoS. It is desirable that an IP-centric wireless broadband access system assign and regulate system and media resources in a manner that can maximize the end-user experience. For some applications such as an initial screen of a Web page download, data transmission speed is the best measure of QoS. For other applications, such as the download or upload of a spreadsheet, the best measure of QoS can be the minimization of transmission error. For some applications, the best measure of QoS can be the optimization of both speed and error. For some applications, the timely delivery of packets can be the best measure of QoS. It is important to note that fast data transmission may not be the same as timely delivery of packets. For instance, data packets that are already "too old" can be transmitted rapidly, but by being too old can be of no use to the user. The nature of the data application itself and the desired end-user experience then can provide the most reliable criteria for the QoS mechanism. It is desired that an IP-centric wireless broadband access system provide a QoS mechanism that can dynamically optimize system behavior to each particular IP flow, and can also adapt to changes with changing network load, congestion and error rates.

4. Service Guarantees and Service Level Agreements (SLAs)

Service guarantees can be made and service level agreements (SLAs) can be entered into between a telecommunications service provider and a subscriber whereby a specified level of network availability can be described, and access charges can be based upon the specified level. Unfortunately, it is difficult to quantify the degree of network availability at any given time, and therefore this becomes a rather crude measure of service performance. It is desired that data delivery rate, error rate, retransmissions, latency, and jitter be used as measures of network availability, but measuring these quantities on a real-time basis can be beyond the capability of conventional network service providers (NSPs).

Another level of service discrimination desired by network service providers is a service level agreement (SLA) that provides for differing traffic rates, network availability, bandwidth, error rate, latency and jitter guarantees. It is desired that an IP-centric wireless broadband access system be provided that can provide for SLAs, enabling service providers to have more opportunities for service differentiation and profitability.

5. Class of Service and Quality of Service

In order to implement a practical QoS mechanism, it is desired that a system be able to differentiate between types of traffic or service types so that differing levels of system resources can be allocated to these types. It is customary to speak of "classes of service" as a means of grouping traffic types that can receive similar treatment or allocation of system and media resources.

Currently, there are several methods that can be used in wireline network devices to implement differentiated service classes. Example methods include traffic shaping, admission control, IP precedence, and differential congestion management. It is desired that an IP-centric wireless broadband access system use all of these methods to differentiate traffic into classes of service, to map these classes of service against a QoS matrix, and thereby to simplify the operation and administration of the QoS mechanism.

B. QoS and IP-Centric Wireless Environment

In a point-to-multipoint (PtMP) wireless system like the present invention, it is desirable that the QoS mechanism cope not only with wireline networking considerations, but also with considerations particular to the wireless environment. As stated earlier, it is desired that the inherent BER of wireless be handled. The high BER can require that error detection, correction, and re-transmission be done in an efficient manner. It is desired that a BER handling mechanism also work efficiently with the re-transmission algorithms of TCP/IP so as to not cause further unnecessary degradation of bandwidth utilization. An additional challenge of wireless is contention among users for limited wireless bandwidth. It is desirable that the system handle service requests from multiple users in a radio medium subject to interference and noise, which can make efficient allocation of radio bandwidth difficult.

As discussed above, the change from circuit-switched and ATM data networks to packet-switched data networks has impacted the definition of QoS mechanisms. The present invention provides a novel QoS mechanism in a point-to-multi-point IP-centric wireless system for packet-switched network traffic. In order for the system to provide optimal QoS performance, it desirable that it include a novel approach to QoS mechanisms. The use of QoS as the underlying guide to system architecture and design constitutes an important, substantial and advantageous difference of the IP-centric wireless broadband access system of the present invention over existing wireless broadband access systems designed with traditional circuit-centric or ATM cell circuit-centric approaches such as those used by Teligent and Winstar.

C. IP-Centric Wireless Broadband Access QoS and Queuing Disciplines

1. Managing Queues

Queuing is a commonly accepted tool required for manipulating data communications flows. In order for packet headers to be examined or modified, for routing decisions to made, or for data flows to be output on appropriate ports, it is desirable that data packets be queued. However, queuing introduces, by definition, a delay in the traffic streams that can be detrimental, and can even totally defeat the intent of queuing. Excessive queuing can have detrimental effects on traffic by delaying time sensitive packets beyond their useful time frames, or by increasing the RTT (Round Trip Time), producing unacceptable jitter or even causing the time-out of data transport mechanisms. Therefore, it is desired that queuing be used intelligently and sparingly, without introducing undue delay in delay-sensitive traffic such as real-time sessions.

In a wireless environment where time division multiple access (TDMA), forward error detection (FEC), and other such techniques can be necessary, it is desirable that queuing be used merely to enable packet and radio frame processing. However, in the case of real-time flows, the overall added delay in real-time traffic can preferably be held to below approximately 20 milliseconds.

The use of queue management as the primary QoS mechanism in providing QoS-based differentiated services is a simple and straight forward method for wireless broadband systems. However, wireless systems are usually more bandwidth constrained and therefore more sensitive to delay than their wireline counterparts. For this reason, it is desirable that QoS-based differentiated services be provided with mechanisms that go beyond what simple queuing can do. However, some queuing can still be required, and the different queuing methods are now discussed.

2. First in, First out (FIFO) Queuing

First in, first out (FIFO) queuing can be used in wireless systems, like wireline systems, in buffering data packets when the downstream data channel becomes temporarily congested. If temporary congestion is caused by bursty traffic, a FIFO queue of reasonable depth can be used to smooth the flow of data into the congested communications segment. However, if the congestion becomes severe in extent, or relatively long in duration, FIFO can lead to the discarding of packets as the FIFO queues are filled to capacity and the network is not capable of accepting additional packets causing discarding of packets, i.e. so-called "packet-tossing." Although this can have a detrimental effect on QoS in and of itself, the discarding of packets may cause future problems with traffic flow as the TCP protocol causes the retransmission of lost packets in the proper sequence, further exacerbating the problem. The problem of packet discards can be minimized by increasing the size of the FIFO buffers so that more time can pass before discards occur. Unfortunately, eventually the FIFO can become large enough that packets can become too old and the round-trip time (RTT) can increase to the point that the packets are useless, and the data connection is virtually lost.

In a wireless broadband environment, the requirement for FIFO queuing is partially dependent upon the type of RF access method being used. For time division multiple access/time division duplex (TDMA/TDD), it can be desirable that data be queued even for collecting enough data for the construction of data frames for transmission. Frequency division multiple access (FDMA) and code-division multiple access (CDMA) are not as "sequential" in nature as TDMA, and therefore have less of a requirement for FIFO queuing. However, generally for all wireless access techniques, noise and interference are factors that can lead to retransmissions, and therefore further delays and consequent adverse effect on QoS.

Using FIFO queuing, shared wireless broadband systems can uniformly delay all traffic. This can seem to be the "fairest" method, but it is not necessarily the best method if the goal is to provide high QoS to users. By using different types of queue management, a much better base of overall QoS can be achieved.

3. Priority Queuing

The shared wireless broadband environment can include a constricted bandwidth segment as data is transmitted over the RF medium. Therefore, regardless of access technique, these systems can require some amount of queuing. However, using FIFO queuing can result in a constant delay to all traffic, regardless of the priority or type of traffic. Most data communications environments can consist of a mixture of traffic, with combinations of real time interactive data, file and data downloads, web page access, etc. Some of these types of traffic are more sensitive to delay, and jitter, than others. Priority queuing simply reorders data packets in the queue based on their relative priorities and types, so that data from more latency- and jitter-sensitive traffic can be moved to the front of the queue.

Unfortunately, if there is downlink data channel congestion, or congestion caused by an overabundance of high priority traffic, the condition of "buffer starvation" can occur. Because of the relative volume of high priority packets consuming a majority of buffer space, little room is left for lower priority packets. These lower priority packets can experience significant delays while system resources are devoted to the high priority packets. In addition to low priority packets being held in buffers for long periods of time, or never reaching the buffers, resulting in significantly delayed data flows for these packets, the actual applications corresponding to these low priority packets can also be disrupted, and stop working. Because of the nature of this queuing approach, overall latency and jitter and RTT for lower priority packets can be unpredictable, having an adverse effect on QoS.

If queue sizes are small, reordering data within the queues can have little beneficial effect on the QoS. In fact, processing required to examine packet headers in order to obtain the information necessary to reorder the queues may itself add significant delay to the data stream. Therefore, particularly for wireless broadband data environments, priority queuing can be not much better than FIFO queuing as a QoS mechanism.

4. Classed Based Queuing

By allocating queue space and system resources to packets based on the class of the packets, buffer starvation can be avoided. Each class can be defined to include of data flows with certain similar priorities and types. All classes can be given a certain minimum level of service so that one high priority data flow cannot monopolize all system resources. With the classification approach, because no data flow is ever completely shut off, the source application can receive information about the traffic rate, and can be able to provide TCP-mediated transmission rate adjustment supporting smooth traffic flow.

Although this approach can work better than FIFO queuing in wireless broadband systems, latency and jitter sensitive flows can still be adversely affected by high priority flows of large volume.

5. Weighted Fair Queuing

A weighted fair queuing method can attempt to provide low-volume flows with guaranteed queuing resources, and can then allow remaining flows, regardless of volume or priority, to have equal amounts of resource. Although this can prevent buffer starvation, and can lead to somewhat better latency and jitter performance, it can be difficult to attain stable performance in the face of rapidly changing RF downlink channel bandwidth availability.

Providing a high quality of service can require a QoS mechanism that is more sophisticated than simple queue management.

D. IP-Centric Wireless Broadband Access QoS and TCP/IP

1. TCP/IP

The TCP/IP protocol stack has become the standard method of transmitting data over the Internet, and increasingly it is becoming a standard in virtual private networks (VPNs). The TCP/IP protocol stack includes not only internet protocol (IP), but also transmission control protocol (TCP), user datagram protocol (UDP), and internet control message protocol (ICMP). By assuming that the TCP/IP protocol stack is the standard network protocol for data communications, the creation of a set of optimal QoS mechanisms for the wireless broadband data environment is more manageable. QoS mechanisms can be created that can span the entire extent of the network, including both the wireline and the wireless portions of the network. These mechanisms can integrate in a smooth and transparent manner with TCP rate control mechanisms and provide end-to-end QoS mechanisms that are adaptive to both the wireline and wireless portions of the network. Of course, segments of the wireline network that are congested or are experiencing other transport problems cannot be solved by a wireless QoS mechanism. However, a wireless QoS mechanism can optimize data flows in a manner that can enhance the end user experience when there is no severe wireline network congestion or bottleneck present.

2. Differentiation by Class

Data traffic can be handled based on classes of service, as discussed above. To differentiate traffic by class, data traffic (or a sequence of data packets associated with a particular application, function, or purpose) can be classified into one of several classes of service. Differentiation can be done on the basis of some identifiable information contained in packet headers. One method can include analyzing several items in, e.g., an IP packet header, which can serve to uniquely identify and associate the packet and other packets from that packet flow with a particular application, function or purpose. As a minimum, a source IP address, a source TCP or UDP port, a destination IP address, and a destination IP or UDP port can serve to associate packets into a common flow, i.e. can be used to classify the packets into a class of service.

By creating a finite and manageable number of discrete classes of service, multiple IP flows can be consolidated and handled with a given set of QoS parameters by the QoS mechanisms. These classes can be defined to provide common and useful characteristics for optimal management in the combined wireline and wireless network segments.

3. Per-Flow Differentiation

A finite and discrete set of classes of service, can enable QoS mechanisms to be less compute-intensive, to use less memory, fewer state machines, and therefore have better scaleability than having individual QoS mechanisms (or sets of parameters) for each individual IP flow. However, in a network access device such as, e.g., a point to multi-point (PtMP) wireless broadband access system, the total number of simultaneous IP flows typically will not exceed the range of 1000, and therefore the amount of processing overhead that could be required could permit a per-flow QoS differentiation without resorting to classes of service. However, class of service consolidation of IP flows provides advantages related to marketing, billing and administration.

Prior to the present invention, per-flow differentiation has not been used in a wireless environment (including radio frequencies transmitted over coaxial cables and satellite communications).

4. Using IP Precedence for Class of Service

IP precedence bits in a type of service (IP TOS) field, as described in Internet Engineering Task Force (IETF)1992b, can theoretically be used as a means to sort IP flows into classes of service. IETF RFC1349 proposed a set of 4-bit definitions with 5 different meanings: minimize delay; maximize throughput; maximize reliability; minimize monetary cost; and normal service.

These definitions could add significantly to networks, routers and access devices in differentiating different types of flow so that resources could be appropriately allocated, resulting in improved QoS. However, the proposal has not been widely used. Several proposals in the IETF could make use of this field, along with resource reservation protocol (RSVP), to improve network handling of packets.

Although the type of service (TOS) field has been an integral component of the TCP/IP specification for many years, the field is not commonly used. Absent appropriate bits in the field being set by a source processor, the access devices, the network and network routers cannot implement QoS mechanisms.

5. TCP-Mediated Transmission Rate Mechanisms

The manner in which TCP governs transmission rate can be incorporated and managed by an IP-centric wireless QoS mechanism. If a TCP mechanism is not managed, any wireless QoS mechanism can be overwhelmed or countered by wireless bandwidth factors. Before addressing the specific wireless factors that can impact TCP transmission speed, a review of TCP transmission rate mechanism is needed.

TCP can control transmission rate by "sensing" when packet loss occurs. Because TCP/IP was created primarily for wireline environment with its extremely low inherent BER, such as those found over fiber optic lines, any packet loss is assumed by TCP to be due to network congestion, not loss through bit error. Therefore, TCP assumes that the transmission rate exceeded the capacity of the network, and responds by slowing the rate of transmission. However, packet loss in the wireless link segment is due primarily to inherently high BER, not congestion. The difference turns out to be not insubstantial.

TCP can initially cause the transmission rate to ramp-up at the beginning of a packet flow, and is called slow-start mode. The rate can be continuously increased until there is a loss or time-out of the packet-receipt acknowledgment message. TCP can then "back-off", can decrease the transmission window size, and then can retransmit lost packets in the proper order at a significantly slower rate. TCP can then slowly increase the transmission rate in a linear fashion, which can be called congestion-avoidance mode.

If multiple users share a wireless radio link as with the present invention, the inherently high BER of the medium could potentially cause frequent packet loss leading to unproductive TCP retransmission in congestion avoidance mode. Because wireless bandwidth can be a precious commodity, a IP-centric wireless QoS mechanism preferably provides for packet retransmission without invoking TCP retransmission and consequent and unnecessary "whipsawing" of the transmission rate. This, along with several other factors, makes desirable creation of an IP-centric wireless media access control (MAC) layer. One function of an IP-centric MAC layer can be to mediate local retransmission of lost packets without signaling TCP and unnecessarily altering the TCP transmission speed. A primary task of the IP-centric wireless MAC layer is to provide for shared access to the wireless medium in an orderly and efficient manner. The MAC layer according to the present invention, Proactive Reservation-based Intelligent Multimedia-aware Media Access (PRIMMA) layer, available from Malibu Networks Inc., of Calabasas, Calif., can also schedule all packet transmissions across the wireless medium on the basis of, e.g., IP flow type, service level agreements (SLAs), and QoS considerations.

6. TCP Congestion Avoidance in an IP-Centric Wireless System

a. Network Congestion Collapse, Global Synchronization and IP-Centric Wireless TCP Congestion Avoidance

The inherently high bit error rate (BER) of wireless transmission can make an occurrence of problems known as congestion collapse or global synchronization collapse more likely than in a wireline environment. When multiple TCP senders simultaneously detect congestion because of packet loss, the TCP senders can all go into TCP slow start mode by shrinking their transmission window sizes and by pausing momentarily. The multiple senders can then all attempt to retransmit the lost packets simultaneously. Because they can all start transmitting again in rough synchrony, a possibility of creating congestion can arise, and the cycle can start all over again.

In the wireless environment, an occurrence of burst noise can cause packet loss from many IP streams simultaneously. The TCP transmission rate mechanisms of the TCP senders can assume that packet loss was due to congestion, and they can all back-off in synchrony. When the TCP senders restart, the senders can restart in rough synchrony, and indeed can now create real congestion in the wireless link segment. This cyclical behavior can continue for some time, and can possibly cause unpredictable system performance. This can be due in part to overflowing system queues which can cause more packets to be dropped and can cause more unproductive retransmissions. This can degenerate into a "race" state that could take many minutes before re-establishing stability; this can have an obvious negative impact on QoS.

In the wireline world, random early detection (RED) can be used to circumvent global synchronization. By randomly selecting packets from randomly selected packet flows before congestion collapse occurs, global synchronization can be avoided. Queues can be monitored, and when queue depth exceeds a preset limit, RED can be activated, activating a synchronously the TCP senders' transmission rate controllers. This can avoid the initial congestion which would otherwise result in collapse and then global synchronization.

Instead of purely random packet discards, the packets to be discarded can be done with consideration to packet priority or type. While still random, the probability of discard for a given flow can be a function of the by packet priority or type. In a wireless system, weighted random early detection (WRED) can be used without the concern of retransmission and TCP rate reset by preferentially selecting UDP packets of real time IP flows such as streaming audio, and H.323 flows with a more critical packet Time-to-Live parameter. These IP flows are more sensitive to latency and jitter, and less sensitive to packet loss.

In the wireless environment, with an appropriately designed MAC layer, packet loss due to BER that might otherwise trigger congestion collapse and global synchronization can best be managed with local retransmission of lost packets according to the present invention and without RED and the unnecessary retransmission of packets by the TCP sender and the resulting reset of TCP transmission rate. The IP-centric wireless system separately manages the TCP transmission window of the TCP sender remotely by transmitting a packet receipt-acknowledgment before the TCP

sender detects a lost packet and initiates retransmission along with an unnecessary reset of the transmission rate. This IP-centric wireless system TCP transmission window manager communicates with the MAC layer in order to be aware of the status of all packets transmitted over the wireless medium.

b. The Effect of Fractal Self-Similar Network Traffic Characteristics vs. Poisson Distributions on Network Congestion

Conventionally, it has been believed that network traffic can be modeled with a Poisson distribution. Using this distribution leads to the conclusion, through system simulations, that the sum of thousands of individual traffic flows with Poisson distributions results in a uniform overall network traffic distribution. In other words, the overall network can "average-out" the burstiness of individual traffic flows. Using this model, network congestion behavior, burst behavior, and dynamic traffic characteristics have been used to create conventional congestion avoidance strategies, design queue buffer sizes in network devices, and traffic and capacity limitation predictions.

More recent studies have demonstrated that TCP/IP-based traffic causes networks to behave in a fractal, or self-similar fashion. With this model, when the burstiness of individual traffic flows is summed for the entire network, the entire network becomes bursty. The bursty nature of network traffic flow is seen over all time scales and flow scales of the network. This has huge implications both in design of an IP-centric wireless broadband system according to the present invention, and in the design of congestion avoidance strategies in the network as a whole. With this new perspective on network behavior, it has become clear that network routers, switches and transmission facilities in many cases have been "under-engineered." This under-engineering has led to a further exacerbation of the congestion behavior of the network.

The implications for IP-centric wireless system architecture and design range from queue buffer capacity to local congestion avoidance strategies. Because wireless systems have the added burden of a high inherent BER, the effect of network-wide congestion behavior on local (wireless media channel) congestion avoidance strategies must be properly gauged and countered. For this reason, it is desirable that congestion avoidance algorithms of the IP-centric wireless system be crafted to optimize traffic flow with new mathematical and engineering considerations that until very recently were not apparent or available to system designers.

With these considerations in mind, IP-centric wireless system design cannot be done with the conventional wireline system design approaches without resulting in very low system performance characteristics. With traditional design approaches of a circuit-centric wireless system, bandwidth utilization, real time multimedia quality, and overall system QoS provide for a dramatically lower end-user experience.

7. Application-Specific Flow Control in an IP-Centric Wireless System

With a range of data flows, each having different bandwidth, latency and jitter requirements, for the achievement of high QoS as perceived by the end user, it is desirable that the IP-centric wireless system be able to manage QoS mechanism parameters over a wide range, and in real time. The QoS mechanism must be able to alter system behavior to the extent that one or more data flows corresponding to specific applications be switched on and off from appropriate end users in a transparent manner. This approach is in contrast to other QoS mechanisms that seek to achieve high QoS by establishing circuit-centric connections from end to end without regard for an underlying application's actual QoS requirements. By using the present invention, providing a QoS mechanism that is application-specific rather than circuit-specific, scarce wireless bandwidth can be conserved and dynamically allocated where needed by the QoS mechanisms associated with each application type.

B. QoS and IP-Centric Wireless Media Access Control

1. Proactive Reservation-based Intelligent Multimedia-aware Media Access (PRIMMA) MAC Layer

The present invention's proactive reservation-based intelligent multimedia-aware media access (PRIMMA) media access control (MAC) layer provides an application switching function of the IP-centric wireless QoS mechanism. Once the nature and QoS requirements of each IP stream are determined by other portions of the system, this information is communicated to the PRIMMA MAC layer so that the IP flows of each application can be switched to appropriate destinations in a proper priority order.

2. PRIMMA IP Protocol Stack Vertical Signaling

For IP streams that originate from a local user's CPE, application-level information about the nature of the application can be used by the system to assign appropriate QoS mechanism parameters to the IP stream. For IP streams that originate from a non-local host, information about the IP streams for use in configuring the appropriate QoS mechanism parameters can be extracted from packet headers. The information about the IP streams is communicated "vertically" in the protocol stack model from the application layer (i.e. OSI level 7) to the PRIMMA MAC layer (i.e. OSI level 2) for bandwidth reservation and application switching purposes. Although this violates the conventional practice of providing isolation and independence to each layer of the protocol stack, thereby somewhat limiting the degree of interchangeability for individual layers of the stack, the advantages far outweigh the negatives in an IP-centric wireless broadband access system.

3. PRIMMA IP Flow Control and Application Switching

Based on a specific set of QoS requirements of each IP application flow in the IP-centric wireless system, applications are switched in a "proactive" manner by appropriate reservations of bandwidth over the wireless medium. The wireless transmission frames in each direction are constructed in a manner dictated by the individual QoS requirements of each IP flow. By using QoS requirements to build the wireless transmission frames, optimal QoS performance can result over the entire range of applications being handled by the system. For example, latency and jitter sensitive IP telephony, other H.323 compliant IP streams, and real-time audio and video streams can be given a higher priority for optimal placement in the wireless transmission frames. On the other hand, hypertext transport protocol (HTTP) traffic, such as, e.g., initial web page transmissions, can be given higher bandwidth reservation priorities for that particular application task. Other traffic without latency, jitter, or bandwidth requirements such as, e.g., file transfer protocol (FTP) file downloads, email transmissions, can be assigned a lower priority for system resources and placement in the wireless transmission frame.

4. PRIMMA TCP Transmission Rate Agent

Wireless end users are separated from a high speed, low BER wireline backbone by a lower speed, high BER wireless segment which can be subject to burst error events. TCP/IP traffic that traverses the wireless segment can experience frequent packet loss that, without intervention, can create congestion collapse and global synchronization as previously discussed. Therefore, it is desirable that the present invention's IP-centric wireless system make use of a TCP transmission rate agent that can monitor packet loss

over the wireless segment, and can manage the remote TCP transmission rate function by recreating and transmitting any lost packet acknowledgments. The PRIMMA MAC layer can itself retransmit any lost packets over the wireless medium.

The IP-centric wireless TCP transmission rate agent or "adjunct" can also flow-control the IP streams when necessary, and in accordance with the QoS requirements of the IP flows. All IP-centric wireless TCP transmission rate agent functionality can be transparent to both local and remote hosts and applications.

F. Telecommunications Networks

1. Voice Network

a. Simple Voice Network

FIG. **1A** is a block diagram providing an overview of a standard telecommunications network **100** providing local exchange carrier (LEC) services within one or more local access and transport areas (LATAs). Telecommunications network **100** can provide a switched voice connection from a calling party **102** to a called party **110**. FIG. **1A** is shown to also include a private branch exchange **112** which can provide multiple users access to LEC services by, e.g., a private line. Calling party **102** and called party **110** can be ordinary telephone equipment, key telephone systems, a private branch exchange (PBX) **112**, or applications running on a host computer. Network **100** can be used for modem access as a data connection from calling party **102** to, for example, an Internet service provider (ISP) (not shown). Network **100** can also be used for access to, e.g., a private data network. For example, calling party **102** can be an employee working on a notebook computer at a remote location who is accessing his employer's private data network through, for example, a dial-up modem connection.

FIG. **1A** includes end offices (EOs) **104** and **108**. EO **104** is called an ingress EO because it provides a connection from calling party **102** to public switched telephone network (PSTN) facilities. EO **108** is called an egress EO because it provides a connection from the PSTN facilities to a called party **110**. In addition to ingress EO **104** and egress EO **108**, the PSTN facilities associated with telecommunications network **100** include an access tandem (AT) (not shown) at points of presence (POPs) **132** and **134** that can provide access to, e.g., one or more inter-exchange carriers (IXCs) **106** for long distance traffic, see FIG. **2A**. Alternatively, it would be apparent to a person having ordinary skill in the art that IXC **106** could also be, for example, a CLEC, or other enhanced service provider (ESP), an international gateway or global point-of-presence (GPOP), or an intelligent peripheral (IP).

FIG. **1A** also includes a private branch exchange (PBX) **112** coupled to EO **104**. PBX **112** couples calling parties **124** and **126**, fax **116**, client computer **118** and associated modem **130**, and local area network **128** having client computer **120** and server computer **122** coupled via an associated modem **130**. PBX **112** is a specific example of a general class of telecommunications devices located at a subscriber site, commonly referred to as customer premises equipment (CPE).

Network **100** also includes a common channel interactive signaling (CCIS) network for call setup and call tear down. Specifically, FIG. **1** includes a Signaling System 7 (SS7) signaling network **114**. Signaling network **114** will be described further below with reference to FIG. **2B**.

b. Detailed Voice Network

FIG. **2A** is a block diagram illustrating an overview of a standard telecommunications network **200**, providing both LEC and IXC carrier services between subscribers located in different LATAs. Telecommunications network **200** is a more detailed version of telecommunications network **100**. Calling party **102***a* and called party **110***a* are coupled to EO switches **104***a* and **108***a*, respectively. In other words, calling party **102***a* is homed to ingress EO **104***a* in a first LATA, whereas called party **110***a* is homed to an egress EO **108***a* in a second LATA. Calls between subscribers in different LATAs are long distance calls that are typically routed to IXCs. Sample IXCs in the United States include AT&T, MCI and Sprint.

Telecommunications network **200** includes access tandems (AT) **206** and **208**. AT **206** provides connection to points of presence (POPs) **132***a*, **132***b*, **132***c* and **132***d*. IXCs **106***a*, **106***b* and **106***c* provide connection between POPs **132***a*, **132***b* and **132***c* (in the first LATA) and POPs **134***a*, **134***b* and **134***c* (in the second LATA). Competitive local exchange carrier (CLEC) **214** provides an alternative connection between POP **132***d* and POP **134***d*. POPs **134***a*, **134***b*, **134***c* and **134***d*, in turn, are connected to AT **208**, which provides connection to egress EO **108***a*. Called party **110***a* can receive calls from EO **108***a*, which is its homed EO.

Alternatively, it would be apparent to a person having ordinary skill in the art that an AT **206** can also be, for example, a CLEC, or other enhanced service provider (ESP), an international gateway or global point-of-presence (GPOP), or an intelligent peripheral.

Network **200** also includes calling party **102***c* homed to CLEC switch **104***c*. Following the 1996 Telecommunications Act in the U.S., CLECs gained permission to compete for access within the local RBOCs territory. RBOCs are now referred to as incumbent local exchange carriers (ILECs).

i. Fixed Wireless CLECs

Network **200** further includes a fixed wireless CLEC **209**. Example fixed wireless CLECs are Teligent Inc., of Vienna, Va., WinStar Communications Inc., Advanced Radio Telecom Corp. And the BizTel unit of Teleport Communications Group Inc. Fixed wireless CLEC **209** includes a wireless transceiver/receiver radio frequency (RF) tower **210** in communication over an RF link to a subscriber transciever RF tower **212**. Subscriber RF tower **212** is depicted coupled to a CPE box, PBX **112***b*. PBX **112***b* couples calling parties **124***b* and **126***b*, fax **116***b*, client computer **118***b* and associated modem **130***b*, and local area network **128***b* having client computer **120***b* and server computer **122***b* coupled via an associated modem **130***b*.

Network **200** also includes called party **110***a*, a fax **116***a*, client computer **118***a* and associated modem **130***a*, and cellular communications RF tower **202** and associated cellular subscriber called party **204**, all coupled to EO **108***a*, as shown.

EO **104***a*, **108***a* and AT **206**, **208** are part of a switching hierarchy. EO **104***a* is known as a class 5 office and AT **208** is a class 3/4 office switch. Prior to the divestiture of the regional Bell Operating Companies (RBOCs) from AT&T following the modified final judgment, an office classification was the number assigned to offices according to their hierarchical function in the U.S. public switched network (PSTN). An office class is a functional ranking of a telephone central office switch depending on transmission requirements and hierarchical relationship to other switching centers. A class 1 office was known as a Regional Center (RC), the highest level office, or the "office of last resort" to complete a call. A class 2 office was known as a Sectional Center (SC). A class 3 office was known as a Primary Center (PC). A class 4 office was known as either a Toll Center (TC) if operators were present, or otherwise as a Toll Point (TP).

A class 5 office was an End Office (EO), i.e., a local central office, the lowest level for local and long distance switching, and was the closest to the end subscriber. Any one center handles traffic from one or more centers lower in the hierarchy. Since divestiture and with more intelligent software in switching offices, these designations have become less firm. Technology has distributed functionality closer to the end user, diffusing traditional definitions of network hierarchies and the class of switches.

ii. Connectivity to Internet Service Providers (ISPs)

In addition to providing a voice connection from calling party **102***a* to called party **110***a*, the PSTN can provide calling party **102***a* a data connection to an ISP (i.e. similar to client **118***b*).

Network **200** can also include an Internet service provider (ISP) (not shown) which could include a server computer **122** coupled to a data network **142** as will be discussed further below with reference to FIG. **1**B. The Internet is a well-known, worldwide network comprising several large networks connected together by data links. These links can include, for example, Integrated Digital Services Network (ISDN), T1, T3, FDDI and SONET links. Alternatively, an internet can be a private network interconnecting a plurality of LANs and/or WANs, such as, for example, an intranet. An ISP can provide Internet access services for subscribers such as client **118***b*.

To establish a connection with an ISP, client **118***b* can use a host computer connected to a modem (modulator/demodulator) **130***b*. The modem can modulate data from the host computer into a form (traditionally an analog form) for transmission to the LEC facilities. Typically, the LEC facilities convert the incoming analog signal into a digital form. In one embodiment, the data is converted into the point-to-point protocol (PPP) format. (PPP is a well-known protocol that permits a computer to establish a connection with the Internet using a standard modem. It supports high-quality, graphical user-interfaces.) As those skilled in the art will recognize, other formats are available, including, e.g., a transmission control program, internet protocol (TCP/IP) packet format, a user datagram protocol, internet protocol (UDP/IP) packet format, an asynchronous transfer mode (ATM) cell packet format, a serial line interface protocol (SLIP) protocol format, a point-to-point (PPP) protocol format, a point-to-point tunneling protocol (PPTP) format, a NETBIOS extended user interface (NETBEUI) protocol format, an Appletalk protocol format, a DECnet, BANYAN/VINES, an internet packet exchange (IPX) protocol format, and an internet control message protocol (ICMP) protocol format.

iii. Communications Links

Note that FIGS. **1**A, **2**A and other figures described herein include lines which may refer to communications lines or which may refer to logical connections between network nodes, or systems, which are physically implemented by telecommunications carrier devices. These carrier devices include circuits and network nodes between the circuits including, for example, digital access and cross-connect system (DACS), regenerators, tandems, copper wires, and fiber optic cable. It would be apparent to persons having ordinary skill in the art that alternative communications lines can be used to connect one or more telecommunications systems devices. Also, a telecommunications carrier as defined here, can include, for example, a LEC, a CLEC, an IXC, an Enhanced Service Provider (ESP), a global or international services provider such as a global point-of-presence (GPOP), and an intelligent peripheral.

EO **104***a* and AT **206** are connected by a trunk. A trunk connects an AT to an EO. A trunk can be called an inter machine trunk (IMT). AT **208** and EO **108***a* are connected by a trunk which can be an IMT.

Referring to FIG. **1**A, EO **104** and PBX **112** can be connected by a private line with a dial tone. A private line can also connect an ISP (not shown) to EO **104**, for example. A private line with a dial tone can be connected to a modem bay or access converter equipment at the ISP. Examples of a private line are a channelized T1 or integrated services digital network (ISDN) primary rate interface (PRI). An ISP can also attach to the Internet by means of a pipe or dedicated communications facility. A pipe can be a dedicated communications facility. A private line can handle data modem traffic to and from an ISP.

Trunks can handle switched voice traffic and data traffic. For example, trunks can include digital signals DS1–DS4 transmitted over T1 –T4 carriers. Table 2 provides typical carriers, along with their respective digital signals, number of channels, and bandwidth capacities.

TABLE 2

Digital signal	Number of channels	Designation of carrier	Bandwidth in Megabits per second (Mbps)
DS0	1	None	0.064
DS1	24	T1	1.544
DS2	96	T2	6.312
DS3	672	T3	44.736
DS4	4032	T4	274.176

Alternatively, trunks can include optical carriers (OCs), such as OC-1, OC-3, etc. Table 3 provides typical optical carriers, along with their respective synchronous transport signals (STSs), ITU designations, and bandwidth capacities.

TABLE 3

Optical carrier (OC) signal	Electrical signal, or synchronous transport signal (STS)	International Telecommunications Union (ITU) terminology	Bandwidth in Megabits per second (Mbps)
OC-1	STS-1		51.84
OC-3	STS-3	STM-1	155.52
OC-9	STS-9	STM-3	466.56
OC-12	STS-12	STM-4	622.08
OC-18	STS-18	STM-6	933.12
OC-24	STS-24	STM-8	1244.16
OC-36	STS-36	STM-12	1866.24
OC-48	STS-48	STM-16	2488.32

As noted, a private line is a connection that can carry data modem traffic. A private line can be a direct channel specifically dedicated to a customer's use between two specified points. A private line can also be known as a leased line. In one embodiment, a private line is an ISDN/primary rate interface (ISDN PRI) connection. An ISDN PRI connection can include a single signal channel (called a data or D channel) on a T1, with the remaining 23 channels being used as bearer or B channels. (Bearer channels are digital channels that bear voice and data information.) If multiple ISDN PRI lines are used, the signaling for all of the lines can be carried over a single D channel, freeing up the remaining lines to carry only bearer channels.

iv. Telecommunications Traffic

Telecommunications traffic can be sent and received from any network node of a telecommunications carrier. A telecommunications carrier can include, for example, a LEC, a CLEC, an IXC, and an Enhanced Service Provider (ESP). In an embodiment, this traffic can be received from a network

node which is, for example, a class 5 switch, such as EO **104***a*, or from a class 3/4 switch, such as AT **206**. Alternatively, the network system can also be, for example, a CLEC, or other enhanced service provider (ESP), an international gateway or global point-of-presence (GPOP), or an intelligent peripheral.

Voice traffic refers, for example, to a switched voice connection between calling party **102***a* and called party **110***a*. It is important to note that this is on a point-to-point dedicated path, i.e., that bandwidth is allocated whether it is being used or not. A switched voice connection is established between calling party **102***a* and EO **104***a*, then to AT **206** then over an IXC's network such as that of IXC **106***a* to AT **208** and then to EO **108***a* and over a trunk to called party **110***a*. In another embodiment, AT **206** or IXC **106***a* can also be, for example, a CLEC, or other enhanced service provider (ESP), an international gateway or global point-of-presence (GPOP), or an intelligent peripheral.

It is possible that calling party **102***a* is a computer with a data connection to a server over the voice network. Data traffic refers, for example, to a data connection between a calling party **102***a* (using a modem) and a server **122***b* that could be part of an ISP. A data connection can be established, e.g., between calling party **102***a* and EO **104***a*, then to AT **206**, then to CLEC **214**, then over a fixed wireless CLEC **209** link to PBX **112***b* to a modem **130***b* associated with server **122***b*.

c. Signaling Network

FIG. 2B illustrates signaling network **114** in greater detail. Signaling network **114** is a separate network used to handle the set up, tear down, and supervision of calls between calling party **102** and called party **110**. Signaling network **114** in the given example is the Signaling System 7 (SS7) network. Signaling network **114** includes service switching points (SSPs) **236, 238, 240** and **242**, signal transfer points (STPS) **222, 224, 226, 228, 230** and **232**, and service control point (SCP) **234**.

In the SS7 network, the SSPs are the portions of the backbone switches providing SS7 functions. The SSPs can be, for example, a combination of a voice switch and an SS7 switch, or a computer connected to a voice switch. The SSPs communicate with the switches using primitives, and create packets for transmission over the SS7 network.

EOs **104***a*, **108***a* and ATs **206, 208** can be respectively represented in SS7 signaling network **114** as SSPs **236, 238, 240** and **242**. Accordingly, the connections between EOs **104***a*, **108***a* and ATs **206, 208** (presented as dashed lines) can be represented by connections **254, 256, 258** and **268**. The types of these links are described below.

The STPs act as routers in the SS7 network, typically being provided as adjuncts to in-place switches. The STPs route messages from originating SSPs to destination SSPs. Architecturally, STPs can and are typically provided in "mated pairs" to provide redundancy in the event of congestion or failure and to share resources (i.e., load sharing is done automatically). As illustrated in FIG. 2B, STPs can be arranged in hierarchical levels, to provide hierarchical routing of signaling messages. For example, mated STPs **222, 224** and mated STPs **226, 228** are at a first hierarchical level, while mated STPs **230, 232** are at a second hierarchical level.

SCPs provide database functions. SCPs can be used to provide advanced features in an SS7 network, including routing of special service numbers (e.g., 800 and 900 numbers), storing information regarding subscriber services, providing calling card validation and fraud protection, and offering advanced intelligent network (AIN) services. SCP **234** is connected to mated STPs **230** and **232**.

In the SS7 network, there are unique links between the different network elements. Table 4 provides definitions for common SS7 links.

Referring to FIG. 2B, mated STP pairs are connected by C links. For example, STPs **222, 224**, mated STPs **226, 228**, and mated STPs **230, 232** are connected by C links (not labeled). SSPs **236, 238** and SSPs **240, 242** are connected by F links **262** and **264**.

Mated STPs **222, 224** and mated STPs **226, 228**, which are at the same hierarchical level, are connected by B links **270, 272, 244** and **282**. Mated STPs **222, 224** and mated STPs **230, 232**, which are at different hierarchical levels, are connected by D links **266,268,274** and **276**. Similarly, mated STPs **226, 228** and mated STPs **230, 232**, which are at different hierarchical levels, are connected by D links **278, 280, 246** and **248**.

SSPs **236, 238** and mated STPs **222, 224** are connected by A links **254** and **256**. SSPs **240, 242** and mated STPs **226, 228** are connected by A links **258** and **260**.

SSPs **236, 238** can also be connected to mated STPs **230, 232** by E links (not shown). Finally, mated STPs **230, 232** are connected to SCP **234** by A links **250** and **252**.

For a more elaborate description of SS7 network topology, the reader is referred to Russell, Travis, Signaling System #7, McGraw-Hill, New York, N.Y. 10020, ISBN 0-07-054991-5, which is incorporated herein by reference in its entirety.

TABLE 4

SS7 link terminology	Definitions
Access (A) links	A links connect SSPs to STPs, or SCPs to STPs, providing network access and database access through the STPs.
Bridge (B) links	B links connect mated STPs to other mated STPs.
Cross (C) links	C links connect the STPs in a mated pair to one another. During normal conditions, only network management messages are sent over C links.
Diagonal (D) links	D links connect the mated STPs at a primary hierarchical level to mated STPs at a secondary hierarchical level.
Extended (E) links	E links connect SSPs to remote mated STPs, and are used in the event that the A links to home mated STPs are congested.
Fully associated (F) links	F links provide direct connections between local SSPs (bypassing STPs) in the event there is much traffic between SSPs, or if a direct connection to an STP is not available. F links are used only for call setup and call teardown.

d. SS7 Signaled Call Flow

To initiate a call in an SS7 telecommunications network, a calling party using a telephone connected to an ingress EO switch, dials a telephone number of a called party. The telephone number is passed from the telephone to the SSP at the ingress EO of the calling party's local exchange carrier (LEC). First, the SSP can process triggers and internal route rules based on satisfaction of certain criteria. Second, the SSP can initiate further signaling messages to another EO or access tandem (AT), if necessary. The signaling information can be passed from the SSP to STPs, which route the signals between the ingress EO and the terminating end office, or egress EO. The egress EO has a port designated by the telephone number of the called party. The call is set up as a direct connection between the EOs through tandem switches if no direct trunking exists or if direct trunking is full. If the call is a long distance call, i.e., between a calling party and a called party located in different local access transport areas (LATAs), then the call is connected through an inter

exchange carrier (IXC) switch. Such a long distance call is commonly referred to as an inter-LATA call. LECs and IXCs are collectively referred to as the public switched telephone network (PSTN).

Passage of the Telecommunications Act of 1996, authorizing competition in the local phone service market, has permitted CLECs to compete with ILECs in providing local exchange services. This competition, however, has still not provided the bandwidth necessary to handle the large volume of voice and data communications. This is due to the limitations of circuit switching technology which limits the bandwidth of the equipment being used by the LECs, and to the high costs of adding additional equipment.

e. Circuit-Switching

Circuit switching dedicates a channel to a call for the duration of the call. Thus, using circuit switching, a large amount of switching bandwidth is required to handle the high volume of voice calls. This problem is compounded by the use of voice circuits to carry data communications over the same equipment that were designed to handle voice communications.

i. Time Division Multiplexed (TDM) Circuit Switching

TDM circuit switching creates a full-time connection or a dedicated circuit between any two attached devices for the duration of the connection. TDM divides the bandwidth down int fixed time slots in which there can be multiple time slots, each with its own fixed capacity, available. Each attached device on the TDM network is assigned a fixed portion of the bandwidth using one or more time slots depending on the need for speed. When the device is in transmit mode, the data is merely placed in this time slot without any extra overhead such as processing or translations. Therefore, TDM is protocol transparent to the traffic being carried. Unfortunately, however, when the device is not sending data, the time slots remain empty, thereby wasting the use of the bandwidth. A higher-speed device on the network can be slowed-down or bottled-up waiting to transmit data, but the capacity that sits idle cannot be allocated to this higher priority device for the duration of the transmission. TDM is not well suited for the bursts of data that are becoming the norm for the data needs in today's organization.

2. Data Network

FIG. 1B depicts an example network **148** including workstations **144** and **146** coupled to data network **142**. Data network **142** can act as a wide area network (WAN) for coupling a plurality of local area networks (LANs) together. Network **148** includes an example local area network including a plurality of host computers such as, e.g., client workstation **138** and server **136**, coupled together by wiring including network interface cards (NICs) and a hub, such as, e.g., an Ethernet hub. The LAN is coupled to data network **142** by a network router **140** which permits data traffic to be routed to workstations **144** and **146** from client **138** and server **136**.

a. Packet-Switching

Unlike voice networks **100** and **200** described above with reference to FIGS. 1A and 2A which transport traffic over circuit-switched connections, data network **148** transports traffic using packet switching.

Currently, internets, intranets, and similar public or private data networks that interconnect computers generally use packet switching technology. Packet switching provides for more efficient use of a communication channel than does circuit switching. Packet switched networks transport packets of information which can include various types of data such as, e.g., digitized voice, data, and video. With packet switching, many different calls can share a communication channel rather than the channel being dedicated to a single call. During a voice call, for instance, digitized voice information might be transferred between the callers only 60% of the time, with silence being transferred the other 40% of the time. With a circuit switched connection, the voice call could tie-up a communications channel that could have 50% of its bandwidth, unused because of the silence. For a data call, information might be transferred between two computers only 10% of the time. With the data call, 90% of the channel's bandwidth may go unused. In contrast, a packet-switched connection would permit the voice call, the data call and possibly other call information to all be sent over the same channel.

Packet switching breaks a media stream into pieces known as, for example, packets, cells or frames. Each packet can then be encoded with address information for delivery to the proper destination and can be sent through the network. The packets can be received at the destination and the media stream is reassembled into its original form for delivery to the recipient. This process is made possible using an important family of communications protocols, commonly called the Internet Protocol (IP).

In a packet-switched network, there is no single, unbroken physical connection between sender and receiver. The packets from many different calls share network bandwidth with other transmissions. The packets can be sent over many different routes at the same time toward the destination, and can then be reassembled at the receiving end. The result is much more efficient use of a telecommunications network's bandwidth than could be achieved with circuit-switching.

b. Routers

Data network **142** can include a plurality of network routers **140**. Network routers are used to route information between multiple networks. Routers act as an interface between two or more networks. Routers can find the best path between any two networks, even if there are several different networks between the two networks.

Network routers can include tables describing various network domains. A domain can be thought of as a local area network (LAN) or wide area network (WAN). Information can be transferred between a plurality of LANs and/or WANs via network routers. Routers look at a packet and determine from the destination address in the header of the packet, the destination domain of the packet. If the router is not directly connected to the destination domain, then the router can route the packet to the router's default router, i.e. a router higher in a hierarchy of routers. Since each router has a default router to which it is attached, a packet can be transmitted through a series of routers to the destination domain and to the destination host bearing the packet's final destination address.

C. Local Area Networks (LANs) and Wide Area Networks (WANs)

A local area network (LAN) can be thought of as a plurality of host computers interconnected via network interface cards (NICs) in the host computers. The NICs are connected via, for example, copper wires so as to permit communication between the host computers. Examples of LANs include an ethernet bus network, an ethernet switch network, a token ring network, a fiber digital data interconnect (FDDI) network, and an ATM network.

A wide area network (WAN) is a network connecting host computers over a wide area. In order for host computers on a particular LAN to communicate with a host computer on another LAN or on a WAN, network interfaces interconnecting the LANs and WANs must exist. An example of a network interface is a router discussed above.

A network designed to interconnect multiple LANs and/or WANs is known as an internet (with a lower case "i"). An internet can transfer data between any of a plurality of networks including both LANs and WANs. Communication occurs between host computers on one LAN and host computers on another LAN via, for example, an internet protocol (IP) protocol. The IP protocol is used to assign each host computer of a network, a unique IP address enabling packets to be transferred over the internet to other host computers on other LANs and/or WANs that are connected to the internet. An internet can comprise a router interconnecting two or more networks.

The "Internet" (with a capital "I") is a global internet interconnecting networks all over the world. The Internet includes a global network of computers which intercommunicate via the internet protocol (IP) family of protocols.

An "intranet" is an internet which is a private network that uses internet software and internet standards, such as the internet protocol (IP). An intranet can be reserved for use by parties who have been given the authority necessary to use that network.

d. Switching vs. Routing

Routing is done at the middle network architecture levels on such protocols as IPX or TCP/IP. Switching is done at a lower level, at layer 2 of the OSI model, i.e. the media access control (MAC) layer.

e. TCP/IP Packet-Centric vs. ATM Circuit-Centric Data Networks

Asynchronous Transfer Mode (ATM) is a fixed-size cell switched circuit-centric data network. ATM implements virtual circuits (VCS), virtual paths (VPs) and transmission paths (TPs). A circuit-centric network like ATM sets up virtual circuits between source and destination nodes which provide QoS by dedicating the virtual circuit to a specific traffic type.

Some networks are packet-centric networks. Unlike a circuit-centric network, a packet-centric network does not use dedicated circuits through which to transfer packets. TCP/IP performs a packetization of user data to be sent between and among the various systems on the IP network. When a large file is sent down the protocol stack, the IP function is responsible for segmentation and packetization of the data. Then a header is placed on the packet for delivery to the data link. The routing and switching of this data is handled at the IP (i.e. network) layer. IP is in a sense a dumb protocol. When a packet is prepared for transmission across the medium, IP does not specifically route the call across a specific channel. Instead, it places a header on the packet and lets the network deal with it. Therefore, the outward bound packets can take various routes to get from a source to a destination. This means that the packets are in a datagram form and not sequentially numbered as they are in other protocols. IP makes its best attempt to deliver the packets to the destination network interface; but it makes no assurances that data will arrive, that data will be free of errors, and that nodes along the way will concern themselves with the accuracy of the data and sequencing, or come back and alert the originator that something is wrong in the delivery mechanism. It is possible that in IP routing of a packet, the packet can be sent along the network in a loop, so IP has a mechanism in its header information to allow a certain number of "hops" or what is called "time to live" on the network. Rather than permit an undeliverable pack to loop around the network, IP has a counter mechanism that decrements every time the packet passes through a network node. If the counter expires, the node will discard the packet. Working together with IP is TCP which provides controls to ensure that a reliable data stream is sent and delivered. At the sending end, TCP puts a byte count header on information that will be delivered to the IP protocol layer and encapsulates it as part of the packet. The receiving end, when it gets packets is responsible for resequencing the packets and ensuring its accuracy. If all of the IP flow is not received correctly, the byte count acknowledgment or nonacknowledgment message can be sent back to the sending end, prompting the sending end to resend the bytes necessary to fill in the remaining portions of the packet flow. TCP buffers additional packets until after resending the nonacknowledged packet.

3. Video Network

FIG. 1C illustrates a conventional video network **150** such as, e.g., a cable television (CATV) network. Video network **150** can include video network **160** coupled to various video capture, distribution links and video output monitors. Video input devices can include, e.g., conference cameras **154** and **158**. Video output devices can include, e.g., televisions **152** and **156**. Video network **160** can include a variety of head end (i.e. the serving end of the cable) and distribution link equipment such as, e.g., coaxial cable television (CATV) and national television standard code (NTSC) tuner equipment for multiplexing various video signals. Standard cable systems have an immense amount of bandwidth available to them.

It is important to note that CATV is a wireless communication method. The frequencies of many video signals are distributed along the cable at the same time. A television tuner selects a particular channel by tuning into a specific frequency or a "frequency band."

Although a cable television CATV video network often includes only one physical cable, a number of channels can simultaneously be present on the cable. This accomplished by sharing the frequency spectrum of the cable and assigning different frequency ranges to different channels using frequency division multiplexing (FDM). A broadband cable communications system can operate exactly like a CATV system. A counter to this FDM technique is division of the cable not divided into frequency bands but into time slots using time-division multiplexing (TDM). With TDM, each transmitting video station can grab the entire bandwidth of the cable, but only for a very short period of time. The cable is currently capable of carrying up to 750 MHz. FDM techniques can be used to divide the channels into a number of dedicated logical channels. Innovations have allowed a time division multiple access (TDMA) within an FDM channel.

A cable system can allow multiplexing on two separate dimensions to achieve data channels over a cable. The channels can be separated by FDM, and in a frequency band the channel can then be shared via TDMA among multiple users. The most common of the TDMA access methods on broadband cable is CSMA/CD developed by XEROX for Ethernet.

Using a single cable, a midsplit arrangement can accommodate two-way simultaneous transmission. Another way to accomodate this is to use a dual cable system.

Broadband is inherently an analog signaling method. Because video cameras, e.g., are also analog devices, a signal from a video camera (or video recorder) can be directly transmitted onto a broadband cable channel in red/green/blue (RGB) format.

G. Convergence of Voice/Data/Video Networks

Recognizing the inherent efficiency of packet-switched data networks such as the Internet, attention has recently focused on the digitization and transmission of voice, data,

video and other information over converged packet-switched data networks. In order to deliver a high quality of service (QoS) end-user experience, the data networks attempt to provide mechanisms to deliver the different types of information timely and with appropriate bandwidth to provide an acceptable end-user experience.

FIG. 2C illustrates an example network **286** carrying voice, data and video traffic over a data network. Network **286** includes calling party **102***b* homed to EO **104***b*, where EO **104***b* is linked to a telephony gateway **288***b*. Network **286** also includes called party **110***c* homed to EO **108***c*, where EO **108***c* is linked to a telephony gateway **288***c*. EOs **104***b* and **108***c* and telephony gateways **288***b* and **288***c* can be linked to signaling network **114**. Telephony gateways **288***b* and **288***c* can also be coupled to data network **142** via routers **140***b* and **140***c*, respectively.

Still referring to FIG. 2C, telephony gateways **288***b* and **288***c* can be used to packetize voice traffic and signaling information into a form appropriate for transport over data network **142**. It would be apparent to those skilled in the art that telephony gateways **288***b* and **288***c* can include various computer devices designed for controlling, setting up and tearing down calls. Voice calls delivered over the data network can include, e.g., voice over packet (VoP), voice over data (VoD), voice over internet protocol (VoIP), voice over asynchronous transfer mode (VoATM), voice over frame (VoF). An example of a telephony gateway **288***b* and **288***c* is a media gateway control protocol (MGCP) compliant gateway available from various vendors such as, e.g., Lucent, of Parsippany, N.J., and CISCO of Palo Alto, Calif. It is important to note that other network devices such as a softswitch available from several member companies of the SoftSwitch Consortium, including Level 3 Communications of Louisville, Colo., could also be necessary to enable transport of, e.g., VoIP.

Network **286** is depicted to include other devices coupled to data network **142**. First, an H.323 compliant video-conferencing system **289** is illustrated including a camera **154***g* and television **152***g* and router **140***g*. Second, a local area network (LAN) **128***a* including a client workstation **138***a* and a server **136***a* are coupled to data network **142** via network router **140***a*. Similarly, LAN **128***f* having a client workstation **138***f* and a server **136***f* are coupled via network router **140***f* to data network **142**.

Data Network **142** can provide for routing of packets of information through network routing devices from source locations to destination locations coupled to data network **142**. For example, data network **142** can route internet protocol (IP) packets for transmission of voice and data traffic from telephony gateway **288***b* to telephony gateway **288***c*. Data Network **142** represents any art-recognized packet centric data network. One well-known data network is the global Internet. Other examples include a private intranet, a packet-switched network, a frame relay network, and an asynchronous transfer mode (ATM) circuit-centric network.

In an example embodiment, data network **142** can be an IP packet-switched network. A packet-switched network such as, e.g., an IP network, unlike a circuit-switched network, does not require dedicated circuits between originating and terminating locations within the packet switched network. The packet-switched network instead breaks a message into pieces known as packets of information. Such packets can then be encapsulated with a header which designates a destination address to which the packet must be routed. The packet-switched network then takes the packets and routes them to the destination designated by the destination address contained in the header of the packet.

Routers **140***a*, **140***b*, **140***c*, **140***d*, **140***e*, **140***f* and **140***g* can be connected to one another via physical media such as, for example, optical fiber link connections, and copper wire connections. Routers **140***a–g* transfer information between one another and intercommunicate according to routing protocols.

Data network **142** could be implemented using any data network such as, e.g., IP networks, ATM virtual circuit-centric networks, frame relay networks, X.25 networks, and other kinds of LANs and WANs. Other data networks could be used interchangeably for data network **142** such as, for example, FDDI, Fast Ethernet, or an SMDS packet switched network. Frame relay and ATM are connection-oriented, circuit-centric services. Switched multi-megabyte data service (SMDS) is a connection-oriented mass packet service that offers speeds up to 45 Mbps.

1. Example Data Networks

a. Asynchronous Transfer Mode (ATM)

ATM is a high-bandwidth, low-delay, fixed-sized cell-based multiplexing network technology. Bandwidth capacity is segmented into 53-byte cells, having a header and payload fields. ATM uses fixed-length cells with the belief that the fixed length cells can be switched more easily in hardware than variable size packets and thus should result in faster transmissions in certain environments.

The ATM environment sets up virtual circuits in a circuit-centric manner. Thus, ATM segments variable length IP packet flows into fixed size cells using a segmentation and resequencing algorithm (SAR).

Each ATM cell contains a 48-byte payload field and a 5-byte header that identifies the so-called "virtual circuit" of the cell. ATM is thought suitable for high-speed combinations of voice, data, and video services. Currently, ATM access can perform at speeds as high as 622 Mbps or higher. ATM has recently been doubling its maximum speed every year.

ATM is defined by a protocol standardized by the International Telecommunications Union (ITU-T), American National Standards Institute (ANSI), ETSI, and the ATM Forum. ATM comprises a number of building blocks, including transmission paths, virtual paths, and virtual channels. Asynchronous transfer mode (ATM) is a cell based switching and multiplexing technology designed to be a general purpose connection-oriented transfer mode for a wide range of telecommunications services. ATM can also be applied to LAN and private network technologies as specified by the ATM Forum.

ATM handles both connection-oriented traffic directly or through adaptation layers, or connectionless traffic through the use of adaptation layers. ATM virtual connections may operate at either a constant bit rate (CBR) or a variable bit rate (VBR). Each ATM cell sent into an ATM network contains a small header including information that establishes a virtual circuit-centric connection from origination to destination. All cells are transferred, in sequence, over this virtual connection. ATM provides either permanent or switched virtual connections (PVCs or SVCs). ATM is asynchronous because the transmitted cells need not be periodic as time slots of data are required to be in synchronous transfer mode (STM).

ATM uses an approach by which a header field prefixes each fixed-length payload. The ATM header identifies the virtual channel (VC). Therefore, time slots are available to any host which has data ready for transmission. If no hosts are ready to transmit, then an empty, or idle, cell is sent.

ATM permits standardization on one network architecture defining a multiplexing and a switching method. Synchro-

nous optical network (SONET) provides the basis for physical transmission at very high-speed rates. ATM can also support multiple quality of service (QoS) classes for differing application requirements by providing separate virtual circuits for different types of traffic, depending on delay and loss performance. ATM can also support LAN-like access to available bandwidth.

Cells are mapped into a physical transmission path, such as the North American DS1, DS3, and SONET; European, E1, E3, and E4; ITU-T STM standards; and various local fiber and electrical transmission payloads. All information is multiplexed and switched in an ATM network via these fixed-length cells.

The ATM cell header field identifies cell type, and priority, and includes six portions. An ATM cell header includes a generic flow control (GFC), a virtual path identifier (VPI), a virtual channel identifier (VCI), a payload type (PT), a call loss priority (CLP), and a header error check (HEC). VPI and VCI hold local significance only, and identify the destination. GFC allows a multiplexer to control the rate of an ATM terminal. PT indicates whether the cell contains user data, signaling data, or maintenance information. CLP indicates the relative priority of the cell, i.e., lower priority cells are discarded before higher priority cells during congested intervals. HEC detects and corrects errors in the header.

The ATM cell payload field is passed through the network intact, with no error checking or correction. ATM relies on higher-layer protocols to perform error checking and correction on the payload. For example, a transmission control protocol (TCP) can be used to perform error correction functions. The fixed cell size simplifies the implementation of ATM switches and multiplexers and enables implementations at high speeds.

When using ATM, longer packets cannot delay shorter packets as in other packet-switched networks, because long packets are separated into many fixed length cells. This feature enables ATM to carry CBR traffic, such as voice and video, in conjunction with VBR data traffic, potentially having very long packets, within the same network.

ATM switches take traffic and segment it into the fixed-length cells, and multiplex the cells into a single bit stream for transmission across a physical medium. As an example, different kinds of traffic can be transmitted over an ATM network including voice, video, and data traffic. Video and voice traffic are very time-sensitive, so delay cannot have significant variations. Data, on the other hand, can be sent in either connection-oriented or connectionless mode. In either case, data is not nearly as delay-sensitive as voice or video traffic. Data traffic, as e.g., spread sheet data requires accurate transmission. Therefore, ATM conventionally must discriminate between voice, video, and data traffic. Voice and video traffic requires priority and guaranteed delivery with bounded delay, while data traffic requires, simultaneously, assurance of low loss. In a converged data network, data traffic can also carry voice traffic, making it also time-dependent. Using ATM, in one embodiment, multiple types of traffic can be combined over a single ATM virtual path (VP), with virtual circuits (VCs) being assigned to separate data, voice, and video traffic.

A transmission path can include one or more VPs. Each VP can include one or more VCs. Thus, multiple VCs can be trunked over a single VP. Switching can be performed on a transmission path, VPs, or at the level of VCs.

The capability of ATM to switch to a virtual channel level is similar to the operation of a private or public branch exchange (PBX) or telephone switch in the telephone world. In a PBX switch, each channel within a trunk group can be switched. Devices which perform VC connections are commonly called VC switches because of the analogy to telephone switches. ATM devices which connect VPs are commonly referred to as VP cross-connects, by analogy with the transmission network. The analogies are intended for explanatory reasons, but should not be taken literally. An ATM cell-switching machine need not be restricted to switching only VCs and cross-connection to only VPs.

At the ATM layer, users are provided a choice of either a virtual path connection (VPC) or a virtual channel connection (VCC). Virtual path connections (VPCs) are switched based upon the virtual path identifier (VPI) value only. Users of a VPC can assign VCCs within a VPI transparently, since they follow the same route. Virtual channel connections (VCCs) are switched upon a combined VPI and virtual channel identifier (VCI) value.

Both VPIs and VCIs are used to route calls through a network. Note that VPI and VCI values must be unique on a specific transmission path (TP).

It is important to note that data network **142** can be any of a number of other data-type networks, including various packet-switched data-type networks, in addition to an ATM network.

b. Frame Relay

Alternatively, data network **142** can be a frame relay network. It would be apparent to persons having ordinary skill in the art, that a frame relay network could be used as data network **142**. Rather than transporting data in ATM cells, data could be transported in frames.

Frame relay is a packet-switching protocol used in WANs that has become popular for LAN-to-LAN connections between remote locations. Formerly frame relay access would top out at about 1.5 Mbps. Today, so-called "high-speed" frame relay offers around 45 Mbps. This speed is still relatively slow as compared with other technology such as ATM.

Frame-relay services employ a form of packet-switching analogous to a streamlined version of X.25 networks. The packets are in the form of frames, which are variable in length. The key advantage to this approach it that a frame relay network can accommodate data packets of various sizes associated with virtually any native data protocol. A frame relay network is completely protocol independent. A frame relay network embodiment of data network **142** does not undertake a lengthy protocol conversion process, and therefore offers faster and less-expensive switching than some alternative networks. Frame relay also is faster than traditional X.25 networks because it was designed for the reliable circuits available today and performs less-rigorous error detection.

c. Internet Protocol (IP)

In an embodiment, data network **142** can be an internet protocol (IP) network over an ATM network. It would be apparent to those skilled in the art, that an internet protocol (IP) network over various other data link layer network suchas, e.g., Ethernet, could be used as data network **142**. Rather than transporting data in fixed length ATM circuit-centric cells, data could be transported in variable length IP datagram packet-centric packets as segmented by TCP. The IP data network can lie above any of a number of physical networks such as, for example, a SONET optical network.

2. Virtual Private Networks (VPNs)

A virtual private network (VPN) is a wide area communications network operated by a telecommunications carrier that provides what appears to be dedicated lines when used, but that actually includes trunks shared among all customers as in a public network. Just as a VPN can be provided as a

service through a wireline network, a VPN can be provided in a wireless network. A VPN can allow a private network to be configured within a public network.

VPNs can be provided by telecommunications carriers to customers to provide secure, guaranteed, long-distance bandwidth for their WANs. These VPNs generally use frame relay or switched multi-megabyte data service (SMDS) as a protocol of choice because those protocols define groups of users logically on the network without regard to physical location. ATM has gained favor as a VPN protocol as companies require higher reliability and greater bandwidth to handle more complex applications. VPNs using ATM offer networks of companies with the same virtual security and QoS as WANs designed with dedicated circuits.

The Internet has created an alternative to VPNs, at a much lower cost, i.e. the virtual private Internet. The virtual private Internet (VPI) lets companies connect disparate LANs via the Internet. A user installs either a software-only or a hardware-software combination that creates a shared, secure intranet with VPN-style network authorizations and encryption capabilities. A VPI normally uses browser-based administration interfaces.

3. H.323 Video Conferencing

The H.323 Recommendation for video conferencing will now be briefly overviewed. The H.323 standard provides a foundation for, for example, audio, video, and data communications across IP-based networks, including the Internet. By complying with the H.323 Recommendation, multimedia products and applications from multiple vendors can interoperate, allowing users to communicate without concern for compatibility. H.323 promises to be the foundation of future LAN-based products multimedia applications.

H.323 is an umbrella recommendation from the International Telecommunications Union (ITU) that sets standards for multimedia communications over Local Area Networks (LANs) that do not provide a guaranteed Quality of Service (QoS). These networks dominate today's corporate desktops and include packet-switched TCP/IP and IPX over Ethernet, Fast Ethernet and Token Ring network technologies. Therefore, the H.323 standards are important building blocks for a broad new range of collaborative, LAN-based applications for multimedia communications.

The H.323 specification was approved in 1996 by the ITU's Study Group 16. Version 2 was approved in January 1998. The standard is broad in scope and includes both stand-alone devices and embedded personal computer technology as well as point-to-point and multipoint conferences. H.323 also addresses call control, multimedia management, and bandwidth management as well as interfaces between LANs and other networks.

H.323 is part of a series of communications standards that enable videoconferencing across a range of networks. Known as H.32X, this series includes H.320 and H.324, which address ISDN and PSTN communications, respectively.

The H.323 architecture defines four major components for network-based communications, including terminals, gateways, gatekeepers, and multipoint control units (MCUs).

Terminals are client endpoints on the LAN that provide real-time, two-way communications. All terminals support voice communications; video and data are optional. H.323 specifies the modes of operation required for different audio, video, and/or data terminals to work together. H.323 is the standard of next generation Internet phones, audio conferencing terminals, and video conferencing technologies.

All H.323 terminals also support H.245, which is used to negotiate channel usage and capabilities. Three other components are required: Q.931 for call signaling and call setup, a component called Registration/Admission/Status (RAS), which is a protocol used to communicate with a gatekeeper; and support for RTP/RTCP for sequencing audio and video packets.

Optional components in an H.323 terminal are video codecs, T.120 data conferencing protocols, and MCU capabilities.

A gateway is an optional element in an H.323 conference. An H.323 gateway can provide many services, the most common being a translation function between H.323 conferencing endpoints and other terminal types. This function includes translation between transmission formats (i.e. H.225.0 to H.221) and between communications procedures (i.e. H.245 to H.242). In addition, a gateway also translates between audio and video codecs and performs call setup and clearing on both the LAN side and the switched-circuit network side.

In general, the purpose of the H.323 gateway is to reflect characteristics of a LAN endpoint to an SCN endpoint and vice versa. The primary applications of gateways are likely to be establishing links with analog PSTN terminals, establishing links with remote H.320 compliant terminals over ISDN-based switched-circuit networks, and establishing links with remote H.324-compliant terminals over PSTN networks.

Gateways are not required if connections to other networks are not needed, since endpoints may directly communicate with other endpoints on the same LAN. Terminals communicate with gateways using the H.245 and Q.931 protocols.

With the appropriate transcoders, H.323 gateways 5806 can support terminals that comply with H.310, H.321, H.322, and V.70.

Many gateway functions are left to the designer. For example, the actual number of H.323 terminals that can communicate through the gateway is not subject to standardization. Similarly, the number of SCN connections, the number of simultaneous independent conferences supported, the audio/video/data conversion functions, and inclusion of multipoint functions are left to the manufacturer. By incorporating H.323 gateway technology into the H.323 specification, the ITU has positioned H.323 as the means to hold standards-based conferencing endpoints together.

The gatekeeper is the most important component of an H.323 enabled network. It can act as the central point for all calls within its zone and provides call control services to registered endpoints. In many ways, an H.323 gatekeeper acts as a virtual switch.

Gatekeepers perform two important call control functions. The first is address translation from LAN aliases for terminals and gateways to IP or IPX addresses, as defined in the RAS specification. The second function is bandwidth management, which is also designated within RAS. For instance, if a network manager has specified a threshold for the number of simultaneous conferences on the LAN, the gatekeeper can refuse to make any more connections once the threshold is reached. The effect is to limit the total conferencing bandwidth to some fraction of the total available; the remaining capacity is left for e-mail, file transfers, and other LAN protocols. A collection of all terminals, gateways, and multipoint control units which can be managed by a single gatekeeper are known as an H.323 Zone.

An optional, but valuable feature of a gatekeeper is its ability to route H.323 calls. By routing a call through a gatekeeper, it can be controlled more effectively. Service

providers need this ability in order to bill for calls placed through their network. This service can also be used to re-route a call to another endpoint if a called endpoint is unavailable. In addition, a gatekeeper capable of routing H.323 calls can help make decisions involving balancing among multiple gateways. For instance, if a call is routed through a gatekeeper, that gatekeeper can then re-route the call to one of many gateways based on some proprietary routing logic.

While a gatekeeper is logically separate from H.323 endpoints, vendors can incorporate gatekeeper functionality into the physical implementation of gateways and MCUs.

A gatekeeper is not required in an H.323 system. However, if a gatekeeper is present, terminals must make use of the services offered by gatekeepers. RAS defines these as address translation, admissions control, bandwidth control, and zone management.

Gatekeepers can also play a role in multipoint connections. To support multipoint conferences, users would employ a gatekeeper to receive H.245 control channels from two terminals in a point-to-point conference. When the conference switches to multipoint, the gatekeeper can redirect the H.245 Control Channel to a multipoint controller, the MC. A gatekeeper need not process the H.245 signaling; it only needs to pass it between the terminals or between the terminals and the MC.

LANs which contain gateways could also contain a gatekeeper to translate incoming E.164 addresses into Transport Addresses. Because a Zone is defined by its gatekeeper, H.323 entities that contain an internal gatekeeper can require a mechanism to disable the internal function so that when there are multiple H.323 entities that contain a gatekeeper on a LAN, the entities can be configured into the same Zone.

The Multipoint Control Unit (MCU) supports conferences between three or more endpoints. Under H.323, an MCU consists of a Multipoint Controller (MC), which is required, and zero or more Multipoint Processors (MP). The MC handles H.245 negotiations between all terminals to determine common capabilities for audio and video processing. The MC also controls conference resources by determining which, if any, of the audio and video streams will be multicast.

The MC does not deal directly with any of the media streams. This is left to the MP, which mixes, switches, and processes audio, video, and/or data bits. MC and MP capabilities can exist in a dedicated component or be part of other H.323 components.

The present invention supports multicast for wireless base station **302**, including providing: compatibility with RFC 1112, 1584; recognition and support of multicasting applications, including: multimedia, teleconferencing, database, distributed computing, real-time workgroups; support of broadcasting function over wireless link; preserves bandwidth, retains QoS latency performance; support of IPv6 IGMP and IPv4 IGMP multicast; group membership query, group membership report messages.

Approved in January of 1998, version 2 of the H.323 standard addresses deficiencies in version 1 and introduces new functionality within existing protocols, such as Q.931, H.245 and H.225, as well as entirely new protocols. The most significant advances were in security, fast call setup, supplementary services and T.120/H.323 integration.

G. Packet-Centric QoS-Aware Wireless Point-to-MultiPoint (PtMP) Telecommunications System

1. Wireless Point-to-MultiPoint Telecommunications System

FIG. 2D depicts network **296** including a point-to-multipoint (PtMP) wireless network **298** coupled via router **140***d* to data network **142**. It is important to note that network **296** includes network **286** from FIG. 2C, plus PtMP wireless network **298**. PtMP wireless network **298** enables customer premise equipment (CPE) at a subscriber location to gain access to the various voice, data and video resources coupled to data network **142** by means of wireless connectivity over a shared bandwidth. The wireless PtMP network **298** is a packet switched network which is TCP/IP packet-centric (i.e. no dedicated circuit is created in delivering a communication IP flow) and QoS aware.

Specifically, PtMP wireless network **298** includes a wireless access point (WAP) **290***d* coupled to router **140***d* by, e.g., a wireline connection. A wireless access point **290***e* can be similarly coupled to router **140***e* by a wireline connection. WAP **290***d* is in wireless communication, such as, e.g., radio frequency (RF) communication, with one or more wireless transciever subscriber antennae **292***d* and **292***e*. It would be apparent to those skilled in the art that various wireless communication methods could be used such as, e.g., microwave, cellular, spread spectrum, personal communications systems (PCS), and satellite.

In an alternative embodiment, RF communication is accomplished over cable television (CATV) coaxial cable. As those skilled in the relevant art will understand, a coaxial cable functions as a waveguide over which RF waves propagate. Accordingly, it is possible for the communications link between RF transceiver subscriber antenna **292***d* and WAP **290***d* to be a coaxial cable. Therefore, a coaxial cable connection is analogous to a wireless connection, and is referred to as an alternative form of wireless connection in the present invention.

In another alternative embodiment, RF communication is accomplished over a satellite connection, such as, e.g., a low earth orbit (LEO) satellite connection or a high earth orbit satellite. Taking the example of an LEO satellite connection, WAP **290***d* and RF transceiver subscriber antenna **292***d* function as satellite gateways, with the additional functionalities described in the present invention.

As would be apparent to those skilled in the art, although the present invention has been described in the context of a point-to-multi-point network, the invention is equally applicable to a point-to-point network environment.

Referring to FIG. 3A, in an embodiment of the invention, WAPs **290***d* and **290***e* can be coupled to a wireless base station **302** where "IP flow" traffic can be queued, analyzed, characterized, classified, prioritized and scheduled, as described more fully below with reference to the ensuing figures.

Referring to FIG. 3B, one embodiment of the invention, antennae **292***d* and **292***e* are coupled to subscriber customer premise equipment (CPE) stations **294***d* and **294***e*, respectively (also referred to as CPEs **294***d*, **294***e*). Subscriber CPE stations **294***d* and **294***e* are coupled to various other CPE equipment via wireline or wireless connections. For example, CPE stations **290***d* and **290***e* can be coupled to voice calling parties **124***d*, **124***e*, **126***d* and **126***e*, fax machines **116***d* and **116***e*, video conferencing equipment including video monitors **152***d* and **152***e*, and cameras **154***d* and **154***e*, host computers including client computers **120***d* and **120***e* and servers **122***d* and **122***e*. Various legacy devices such as PBXs can be coupled to CPEs **294***d* and **294***e*. In addition, next generation technologies such as Ethernet phones available from Selsius, a subsidiary of CISCO Systems from San Jose, Calif. and other Internet appliances can be coupled via LAN connections to CPEs **294***d* and **294***e*. Other video conferencing equipment as well as H.323 compliant conferencing equipment can also be coupled to CPEs **294***d* and **294***e*.

In an embodiment of the invention, either of antennae **292***d* and **292***e* can communicate with both WAPs **290***d* and **290***e* for alternate or backup wireless communications paths.

Returning to FIG. **3**A, it depicts an example perspective diagram **300** of a PtMP network of the present invention. Diagram **300** includes a wireless base station **302** shown in wireless communication with subscriber locations **306***a*, **306***b*, **306***c*, **306***d*, **306***e*, **306***f*, **306***g*, **306***h*, **306***i* and **306***j*. Specifically, wireless base station **302** communicates via wireless access point **290***d* to subscriber antennae **292***a–j* of subscriber locations **306***a–j*.

Wireless base station **302** is coupled at interface **320** to network router **140***d* by, e.g., a wireline connection. Network router **140***d* is coupled to data network **142** which includes various other network routers **140***b* for routing traffic to other nodes on data network **142** such as, e.g., telephony gateway **288***b*.

Returning to FIG. **3**B, it depicts block diagram **310** further illustrating the wireless PtMP of the present invention. Diagram **310** includes wireless base station **302** coupled at interface **320** to data network **142**. Also coupled to data network **142** are router **140***d* and telephony gateway **288***b* which is in turn coupled to a class central office (CO) switch at EO **104***b*. IP telephony gateway **288***b* can terminate telephony traffic to PSTN facilities by, e.g., translating packets into time domain multiplexed (TDM) standard telephone signals. Wireless base station **302** is in communication with wireless CPE **294***d* at subscriber location **306***d* via antenna WAP **290***d* and **292***d*. It would be apparent to those skilled in the art that other configurations of CPE **294***d* are possible, such as, e.g., one or more host computers with no telephone devices, one or more telephones with no host computers, one or more host computers and one or more telephone devices, and one or more H.323 capable videoconferencing platforms which could include a host computer with monitor and camera.

CPE **294***d* is shown with several telephone devices **124***d* and **126***d*, e.g., analog phones, and host computers, client **120***d* and server **122***d*. Client **120***d* and server **122***d* can be coupled to CPE **294***d* via a LAN connection such as, e.g., an Ethernet LAN, or via a legacy V.35 device **322***d* providing a high speed data connection. Other Internet appliances capable of attachment to a data network can also be coupled to CPE **294***d*.

2. Networking Protocol Stack Architecture—Wireless IP Network Access Architecture (WINAAR)

FIG. **4** depicts the wireless IP network access architecture (WINAAR) **400** of the present invention. Architecture **400** illustrates the networking protocol stack which is a version of a TCP/IP protocol stack enhanced to support IP-centric, QoS over a packet switched, shared bandwidth, wireless PtMP connection. The networking protocol stack will be described in terms of the Open Systems Interconnect (OSI) 7 layer networking protocol stack standard which includes physical layer (OSI layer 1) **402**, data link layer (OSI layer 2) **404**, network layer (OSI layer 7) **406** and **408**, transport layer (OSI layer 4) **410** and applications layer (OSI layer 7) **412**.

a. Physical Layer

In an example embodiment, physical layer **402** can be implemented using several wireless application specific integrated circuits (wASICs), an off-the-shelf 16QAM/QPSK **416** ASIC; an Interference Mitigation and Multipath Negation (IMMUNE)/RF **418** algorithm ASIC for minimizing and/or eliminating harmful interference; and a frequency hopping (FH) **419** ASIC for providing dynamic and adaptive multi-channel transmission that optimizes data link integrity by changing frequency levels depending on the noise level of a given frequency. Physical layer **402** can include the radio frequency (RF) signal **415**.

b. Data Link Layer

Data link layer **404** lies on top of physical layer **402**. Data link layer **404** can include a media access control (MAC) layer **414** which is depicted graphically in diagram **400** as MAC layer portion **414***a* and proactive reservation-based intelligent multi-media access (PRIMMA) technology portions **414***b* and **414***c*. Arrows **426**, **428** and **430**, respectively, illustrate that MAC layer **414** can read header information from data and multimedia applications **425**, TCP/UDP **427** and IP **429** layers to analyze and schedule an IP packet of an "IP flow." IP packets of the IP flow are identified by analyzing the header information to determine QoS requirements of the IP flow, so that the IP flow can be characterized, classified, presented, prioritized and scheduled.

c. Network Layer

1. Internet Protocol (IP)

Network layer **408** is the Internet protocol (IP) **429**. As will be discussed further below and as already discussed above with reference to data network **142**, IP is a standard protocol for addressing packets of information. Referring now to FIG. **7**, IP header fields **702** can include, e.g., source and destination IP addresses, IP type of service (TOS), IP time to live (TTL), and protocol fields. IP is a datagram protocol that is highly resilient to network failures, but does not guarantee sequence delivery. Routers send error and control messages to other routers using the Internet control message protocol (ICMP). ICMP can also provide a function in which a user can send a "ping" (echo packet) to verify reachability and round trip delay of an IP-addresse host. Another OSI layer **3** protocol is address resolution protocol (ARP) which can directly interface to the data link layer. ARP maps a physical address, e.g., an Ethernet MAC address, to an IP address.

2. Internet Protocol (IP)v4 and IPv6

IP **429** of network layer **408** can be, e.g., an IP version 4 (IPv4) or an IP version 6 (IPv6). IPv6 (sometimes called next-generation internet protocol or IPng) is a backward-compatible extension of the current version of the Internet protocol, IPv4. IPv6 is designed to solve problems brought on by the success of the Internet (such as running out of address space and router tables). IPv6 also adds needed features, including circuiting security, auto-configuration, and real-time services similar to QoS. Increased Internet usage and the allocation of many of the available IP addresses has created an urgent need for increased addressing capacity. IPv4 uses a 32-byte number to form an address, which can offer about 4 billion distinct network addresses. In comparison, IPv6 uses 128-bytes per address, which provides for a much larger number of available addresses.

3. Resource Reservation Protocol (RSVP)

IP **429** of network layer **408** can have RSVP enhancement. Developed to enhance IPv4 with QoS features, RSVP is supposed to let network managers allocate bandwidth based on the bandwidth requirements of an application. Basically, RSVP is an emerging communications protocol that is hoped to signal a router to reserve bandwidth for real-time transmission of data, video, and audio traffic.

Resource reservation protocols that operate on a per-connection basis can be used in a network to elevate the priority of a given user temporarily. RSVP runs end to end to communicate application requirements for special handling. RSVP identifies a session between a client and a server and asks the routers handling the session to give its communications a priority in accessing resources. When the

session is completed, the resources reserved for the session are freed for the use of others.

RSVP unfortunately offers only two levels of priority in its signaling scheme. Packets are identified at each router hop as either low or high priority. However, in crowded networks, two-level classification may not be sufficient. In addition, packets prioritized at one router hop might be rejected at the next.

Accepted as an IETF standard in 1997, RSVP does not attempt to govern who should receive bandwidth, and questions remain about what will happen when several users all demand a large block of bandwidth at the same time. Currently, the technology outlines a first-come, first-served response to this situation. The IETF has formed a task force to consider the issue.

Because RSVP provides a special level of service, many people equate QoS with the protocol. For example, Cisco currently uses RSVP in its IPv4 -based internetwork router operating system to deliver IPv6 -type QoS features. However, RSVP is only a small part of the QoS picture because it is effective only as far as it is supported within a given client/server connection. Although RSVP allows an application to request latency and bandwidth, RSVP does not provide for congestion control or network-wide priority with the traffic flow management needed to integrate QoS across an enterprise. Further, RSVP does not address the particular challenges related to delivering packets over a wireless medium.

The present invention supports RSVP by providing: (1) compatibility with RFC **2205**; (2) recognition and support of RSVP messages, including: Path messages, Reservation (Resv), Path teardown messages, Resv teardown messages, Path error messages, Resv error messages, and Confirmation messages; (3) recognition and support of RSVP objects, including: Null, Session, RSVP_Hop, Time_Values, Style, Flowspec, Sender_Template, Sender_Tspec, Adspec, Error_Spec, Policy_Data, Integrity, and Scope, Resv_Confirm; (4) configurable translation of RSVP Flowspecs for QoS resource allocation in wireless base station **302**.

The present invention provides support of DiffServ and RSVP/int-serv by providing: (1) support of RFC **2474** and **2475**; (2) DiffServ in the core of Internet; (3) RSVP/int-serv for hosts and edge networks; (4) admission control capability for DiffServ compatibility; (5) differentiated services (DSs) (a field marking supported for use by DiffServ, and translation into a wireless base station **302** resource allocation); and (6) support for binding of multiple end-to-end sessions to one tunnel session.

4. Real-time Transport Protocol (RTP) and Real-time Control Protocol (RTCP)

TCP of transport layer **410** can have a RTP and RTCP enhancement. Real-time transport protocol (RTP) is an emerging protocol for the Internet championed by the audio/video transport workgroup of the IETF. Referring to FIG. 7, RTP and RTCP header fields **708** can include several sub fields of information. RTP supports real-time transmission of interactive voice and video over packet-switched networks. RTP is a thin protocol that provides content identification, packet sequencing, timing reconstruction, loss detection, and security. With RTP, data can be delivered to one or more destinations, with a limit on delay.

RTP and other Internet real-time protocols, such as the Internet stream protocol version 2 (St2), focus on the efficiency of data transport. RTP and other Internet real-time protocols like RTCP are designed for communications sessions that are persistent and that exchange large amounts of data. RTP does not handle resource reservation or QoS control. Instead, RTP relies on resource reservation protocols such as RSVP, communicating dynamically to allocate appropriate bandwidth.

RTP adds a time stamp and a header that distinguishes whether an IP packet is data or voice, allowing prioritization of voice packets, while RSVP allows networking devices to reserve bandwidth for carrying unbroken multimedia data streams.

Real-time Control Protocol (RTCP) is a companion protocol to RTP that analyzes network conditions. RTCP operates in a multi-cast fashion to provide feedback to RTP data sources as well as all session participants. RTCP can be adopted to circumvent datagram transport of voice-over-IP in private IP networks. With RTCP, software can adjust to changing network loads by notifying applications of spikes, or variations, in network transmissions. Using RTCP network feedback, telephony software can switch compression algorithms in response to degraded connections.

5. IP Multi-Casting Protocols

IP **429** of network layer **408** can also support multi-casting protocols. Digital voice and video comprise of large quantities of data that, when broken up into packets, must be delivered in a timely fashion and in the right order to preserve the qualities of the original content. Protocol developments have been focused on providing efficient ways to send content to multiple recipients, transmission referred to as multi-casting. Multi-casting involves the broadcasting of a message from one host to many hosts in a one-to-many relationship. A network device broadcasts a message to a select group of other devices such as PCS or workstations on a LAN, WAN, or the Internet. For example, a router might send information about a routing table update to other routers in a network.

Several protocols are being implemented for IP multi-casting, including upgrades to the Internet protocol itself. For example, some of the changes in the newest version of IP, IPv6, will support different forms of addressing for uni-cast (point-to-point communications), any cast (communications with the closest member of a device group), and multi-cast. Support for IP multi-casting comes from several protocols, including the Internet group management protocol (IGMP), protocol-independent multi-cast (PIM) and distance vector multi-cast routing protocol (DVMRP). Queuing algorithms can also be used to ensure that video or other multi-cast data types arrive when they are supposed to without visible or audible distortion.

Real-time transport protocol (RTP) is currently an IETF draft, designed for end-to-end, real-time delivery of data such as video and voice. RTP works over the user datagram protocol (UDP), providing no guarantee of in-time delivery, quality of service (QoS), delivery, or order of delivery. RTP works in conjunction with a mixer and translator and supports encryption and security. The real-time control protocol (RTCP) is a part of the RTP definition that analyzes network conditions. RTCP provides mandatory monitoring of services and collects information on participants. RTP communicates with RSVP dynamically to allocate appropriate bandwidth.

Internet packets typically move on a first-come, first-serve basis. When the network becomes congested, Resource Reservation Protocol (RSVP) can enable certain types of traffic, such as video conferences, to be delivered before less time-sensitive traffic such as E-mail for potentially a premium price. RSVP could change the Internet's pricing structure by offering different QoS at different prices. Using SLAs, different QoS levels can be provided to users at CPE location stations depending on SLA subscription level.

The RSVP protocol can be used by a host, on behalf of an application, to request a specific QoS from the network for particular data streams or flows. Routers can use the RSVP protocol to deliver QoS control requests to all necessary network nodes to establish and maintain the state necessary to provide the requested service. RSVP requests can generally, although not necessarily, result in resources being reserved in each node along the data path.

RSVP is not itself a routing protocol. RSVP is designed to operate with current and future uni-cast and multi-cast routing protocols. An RSVP process consults the local routing database to obtain routes. In the multi-cast case for example, the host sends IGMP messages to join a multi-cast group and then sends RSVP messages to reserve resources along the delivery paths of that group. Routing protocols determine where packets are forwarded. RSVP is concerned with only the QoS of those packets as they are forwarded in accordance with that routing. The present invention delivers QoS-aware wireless PtMP access to users over a shared wireless bandwidth, and can take into account priority information provided within packet headers of packets in IP flows received for transmission over the wireless base station's bandwidth.

d. VPN Networks (Example Optional Protocols) at Network Layer

Also at network layer **406** are depicted example optional virtual private network (VPN) protocols point to point protocol (PPP) **420** and IPsec **422**, discussed below.

A plurality of protocol standards exist today for VPNs. For example, IP security (IPsec), point-to-point tunneling protocol (PPTP), layer 2 forwarding protocol (L2F) and layer 2 tunneling protocol (L2TP). The IETF has proposed a security architecture for the Internet protocol (IP) that can be used for securing Internet-based VPNs. IPsec facilitates secure private sessions across the Internet between organizational firewalls by encrypting traffic as it enters the Internet and decrypting it at the other end, while allowing vendors to use many encryption algorithms, key lengths and key escrow techniques. The goal of IPsec is to let companies mix-and-match the best firewall, encryption, and TCP/IP protocol products.

IPsec is designed to link two LANs together via an encrypted data stream across the Internet.

1. Point-to-Point Tunneling Protocol (PPTP)

Point-to-point tunneling protocol (PPTP) provides an alternate approach to VPN security than the use of IPsec. Unlike IPsec, which is designed to link two LANs together via an encrypted data stream across the Internet, PPTP allows users to connect to a network of an organization via the Internet by a PPTP server or by an ISP that supports PPTP. PPTP was proposed as a standard to the IETF in early 1996. Firewall vendors are expected to support PPTP.

PPTP was developed by Microsoft along with 3Com, Ascend and US Robotics and is currently implemented in WINDOWS NT SERVER 4.0, WINDOWS NT WORKSTATION 4.0, WINDOWS 95 via an upgrade and WINDOWS 98, available from Microsoft Corporation of Redmond, Wash.

The "tunneling" in PPTP refers to encapsulating a message so that the message can be encrypted and then transmitted over the Internet. PPTP, by creating a tunnel between the server and the client, can tie up processing resources.

2. Layer 2 Forwarding (L2F) Protocol

Developed by Cisco, layer 2 forwarding protocol (L2F) resembles PPTP in that it also encapsulates other protocols inside a TCP/IP packet for transport across the Internet, or any other TCP/IP network, such as data network **112**. Unlike PPTP, L2F requires a special L2F-compliant router (which can require changes to a LAN or WAN infrastructure), runs at a lower level of the network protocol stack and does not require TCP/IP routing to function. L2F also provides additional security for user names and passwords beyond that found in PPTP.

3. Layer 2 Tunneling Protocol (L2TP)

The layer 2 tunneling protocol (L2TP) combines specifications from L2F with PPTP. In November 1997, the IETF approved the L2TP standard. Cisco is putting L2TP into its Internet operating system software and Microsoft is incorporating it into WINDOWS NT 5.0. A key advantage of L2TP over IPsec, which covers only TCP/IP communications, is that L2TP can carry multiple protocols. L2TP also offers transmission capability over non-IP networks. L2TP however ignores data encryption, an important security feature for network administrators to employ VPNs with confidence.

4. IPsec

IP flows using the security encryption features of IPsec **422** are supported by the present invention. The integration of IPsec **422** flows of WINAAR architecture **400** are described below in the downlink and uplink directions with reference to FIGS. **17**A and **17**B, respectively. Wireless base station **302** supports prioritization of IPsec encrypted streams by placing the iS firewall at the wireless base station and unencrypting the datastream and packet header information prior to identification analysis. Through the wireless transmission medium, the frame stream already includes encryption of the frame data and implements frequency hopping.

IPsec provides for secure data transmission for, e.g., VPNs and eCommerce security. IPsec is compatible with RFC 2401–2407. IPsec is supported with IPv4 and IPv6, and also IPsec tunnel mode. Wireless base station **302** security protocol support includes authentication header (AH) and encapsulating security payload (ESP). Wireless base station **302** supports–IPsec authentication (MD5), encryption algorithms, and automatic key management (IKE and ISAKMP/Oakley). Wireless base station **302** provides for a choice of transport mode or tunnel mode and selectable granularity of security service, such as, e.g., providing a single encrypted tunnel for all traffic between two hosts, or providing separate encrypted tunnel for each TCP connection between hosts.

e. Transport Layer

1. Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol/Internet Protocol (UDP/IP)

As already discussed, internet protocol (IP) has become the primary networking protocol used today. This success is largely a part of the Internet, which is based on the transmission control protocol/internet protocol (TCP/IP) family of protocols. TCP/IP is the most common method of connecting PCs, workstations, and servers. TCP/IP is included as part of many software products, including desktop operating systems (e.g., Microsoft's Windows 95 or Windows NT) and LAN operating systems.

The most pervasive LAN protocol to date, has been IPX/SPX from Novell's NetWare network operating system (NOS). However, IPX/SPX is losing ground to TCP/IP. Novell now incorporates native IP support into NetWare, ending NetWare's need to encapsulate IPX packets when carrying them over TCP/IP connections. Both UNIX and Windows NT servers can use TCP/IP. Banyan's VINES, IBM's OS/2 and other LAN server operating systems can also use TCP/IP.

Transport layer four **410** can include transmission control protocol (TCP) or user datagram protocol (UDP) **427** part of

the standard TCP/UDP/IP protocol family suite of networking protocols. As will be discussed further below and as already mentioned briefly above with reference to data network **142**, TCP is a standard protocol for segmenting traffic into packets, transmitting, reassembling and retransmitting packets of information between a source and destination IP address. Referring now to FIG. **7**, TCP header fields **706** can include, e.g., source and destination port numbers, window size, urgent pointer, flags (SYN, ISN, PSH, RST, FIN), and maximum segment size (MSS). Both TCP and UDP provide a capability for the TCP/IP host to distinguish among multiple applications through port numbers. TCP can provide for a reliable, sequenced delivery of data to applications. TCP can also provide adaptive flow control, segmentation, and reassembly, and prioritization of data flows. UDP only provides unacknowledged datagram capability. The recently defined real time protocol (RTP), RFC 1889, can provide real time capabilities in support of multimedia applications, for example.

TCP uses a window-based flow control. Each TCP source has a dynamically changing transmit window that determines how many packets it can transmit during each successive round-trip time (RTT). The TCP source can continue increasing its transmit window if no packets were lost within the last RTT. Once congestion is detected, the source TCP throttles back its transmission, i.e. it "backs-off," via a multiplicative decrease. An increasing width of the so-called TCP window versus time corresponds to increasingly longer bursts of packets. TCP's window flow-controlled protocol exhibits this effect of increasing throughput and buffer utilization until terminated by loss, followed by a period of rapid backoff.

TCP works over IP to provide end-to-end reliable transmission of data across data network **142**. TCP controls the amount of unacknowledged data in transit by dynamically reducing either window size or segment size. The reverse is also true in that increased window or segment size values achieve higher throughput if all intervening network elements have low error rates, support the larger packets, and have sufficient buffering to support larger window sizes.

f. Application Layer

Applications layer seven **412** can include applications **426** such as, e.g., over TCP, hypertext transport protocol (HTTP), file transfer protocol (FTP), TELNET remote terminal login, and simple simple mail transfer protocol (SMTP); and over UDP, simple network management protocol (SNMP), RPC, NFS, and TFTP. Other applications can also run over the network stack such as, e.g., a world wide web browser such as NETSCAPE NAVIGATOR available from AOL of Reston, Va., a spreadsheet application program such as LOTUS 123 available from IBM of Armonk, N.Y. or a video teleconferencing program such as MS NetMeeting available from MICROSOFT of Redmond, Wash. Packets transmitted from such applications could require special handling and prioritization to achieve an appropriate end-user QoS.

3. PRIMMA-System IP Flow Prioritization

a. Scheduling of Mixed IP Flows

FIG. **6** illustrates block diagram **600** representing scheduling of mixed IP flows. Block diagram **600** shows the scheduling of wireless base station **302**. The functionality of block diagram **600** includes PRIMMA management of Internet, VPN, and realtime IP flows. Referring back to FIG. **3A**, wireless IP flows are coming from data network **142** via network router **140***d* to interface **320** of wireless base station **302**. IP flows are then scheduled for transmission from wireless base station **302** via antenna **290***d* through subscriber location **306***d* via antenna **292***d*.

Referring back to block diagram **600** of FIG. **6**, illustrated therein are the downlink and uplink flows between interface **320** and wireless base station antenna **290***d*. An IP flow, as described herein, refers to a series of related packets of data transmitted from a source to a destination post computer. IP flow **630** from data network **142** (over interface **320**) comprises Internet IP flows **608**, VPN IP flows **610**, and realtime IP flows **612**. IP flow **630** is in the downlink direction.

Downlink IP flow analyzer **602** (hereinafter downlink flow analyzer **602**) analyzes Internet IP flow **608**, VPN IP flow **610** and realtime IP flow **612**. IP flow analyzer **602** is described further below with reference to FIGS. **8A** and **15A**. IP flow analyzer **602** receives packets and analyzes packet header fields to identify new or existing IP flows. IP flow analyzer **602** can also characterize QoS requirements for the IP flow depending on packet header field contents. IP flow analyzer **602** can classify the IP flow and associate a given packet with other packets from an existing IP flow and can group together IP flows with similar QoS requirements. IP flow analyzer **602** can also present the IP flows to a flow scheduler.

Downlink PRIMMA MAC IP flow scheduler **604** (hereinafter downlink flow scheduler **604**) schedules received IP flows **608**, **610**, and **612** for transmission in the downlink direction. Downlink flow scheduler **604** can prioritize the different classes of IP flows. For example, scheduler **604** can reserve slots in downlink frames for latency sensitive IP flows; for FTP type IP flows **608**, scheduler **604** can allocate large amounts of bandwidth for file transfer; and for e-mail type IP flows **608**, a lower priority can be given to packets. In prioritizing allocation of wireless bandwidth frame slots, downlink flow scheduler **604** can take into account the fact that an IP flow **630** is a VPN IP flow **610** from a virtual private network (VPN), such as, e.g., a remote branch office tieing into a corporate network. All traffic from a VPN can be given a higher priority or specific types of VPN traffic can request particular service levels. Downlink flow scheduler **604** can prioritize realtime IP flows **612** such that their arrival at CPEs **294** at CPE subscriber locations **306** will occur as required.

Downlink PRIMMA MAC segmentation and resequencing (SAR) and framer **606** (hereinafter downlink SAR and framer **606**) segments and frames the data packets of received IP flows into frames for transmission over the wireless medium to CPEs **294** at CPE subscriber locations **306**. For example IP flow **616**, **624** can be transmitted to CPE **294***d* at CPE subscriber location **306***d*, via base station antenna **290***d* over a wireless medium to subscriber antenna **292***d* and CPE **294***d* at CPE subscriber location **306***d*. In the present invention, the term wireless medium is used to broadly encompass not only propagation of RF transmissions over cellular communications, but also RF transmissions over satellite communications and cable (e.g., coaxial cable) communications.

In the uplink direction, IP flow **626** from CPE **294***d* at CPE subscriber station **306***d* is received at wireless base station antenna **290***d*. IP flow **626** can include Internet IP flow **618**, VPN IP flow **620** and realtime IP flow **622**. Uplink IP flow analyzer **632** (hereinafter uplink flow analyzer **632**) analyzes Internet IP flow **618**, VPN IP flow **620** and realtime IP flow **622**. Uplink flow analyzer **632** is described further below with reference to FIGS. **8B** and **15B**. In one embodiment, the functionality of IP flow analyzer **632** occurs at the CPE **294***d* at subscriber CPE location **306***d* and sends a request to transmit data up to wireless base station **302**, including information about an IP flow for which CPE **294***d* would like to schedule an uplink slot.

Uplink PRIMMA MAC IP flow scheduler **634** (hereinafter uplink flow scheduler **634**) can schedule the requested IP flow. In one embodiment, the functionality of scheduler **634** can be performed at CPE **294***d* at subscriber CPE location **306***d*. In another embodiment, the functionality of scheduler **634** can be performed at the wireless base station **302**. An advantage of placing uplink flow scheduler **634** at the wireless base station is that this provides efficiencies particularly in a point-to-multi-point architecture. It is more efficient to have one centralized scheduler at the base station **302** rather than to place multiple uplink flow schedulers **634** at CPEs **294** of subscriber CPE locations **306**.

Uplink PRIMMA MAC segmentation and resequencing (SAR) and framer **636** (hereinafter SAR and framer **636**) can segment and frame the data packets of IP flows into frames for transmission over the wireless medium from CPE **294** at CPE subscriber locations **306** to wireless base station **302** for further transmission over data network **142**. IP flow **626** from CPE **294***d* at CPE subscriber location **306***d* can be transmitted to base station antenna **290***d* over a wireless medium such as, e.g., RF communication, cable modem and satellite communication, from subscriber antenna **292***d* coupled to CPE **294***d* at CPE subscriber location **306***d*.

b. Summary of Downlink and Uplink SubFrame Prioritization

Block diagram **800** of FIG. **8**A summarizes an exemplary downlink analysis, prioritization and scheduling function. Similarly, block diagram **830** of FIG. **8**B summarizes an exemplary uplink analysis prioritization and scheduling function. Block diagram **800** and **830** are more detailed views of the function of block diagram **600** of FIG. **6**.

Beginning with block diagram **800** (of FIG. **8**A), it depicts how IP flow prioritization and scheduling of a shared wireless bandwidth is performed in the downlink path, from data network **142**—to router **140***d*—to interface **320**—to wireless base station **302**—WAP **290***d*—over a wireless medium—to wireless transceiver subscriber antenna **292***d*—to subscriber CPE station **294***d* at subscriber CPE location **306***d*.

IP flow analyzer **602** performs the function of identifying, characterizing, classifying, and presenting data packets to a downlink frame scheduler. The functions of identifying, characterizing, classifying and presenting the data packets are described with respect to FIG. **15**A.

During identification, it is determined whether a data packet of an incoming IP data flow is known to the system, i.e. is an "existing IP flow", or rather is the first data packet of a new IP data flow, based on fields in a packet header section. Identification can also include, e.g., determining the source of the packet in order to extrapolate the type of information in the packet payload.

During characterization, a new data packet (of a new IP data flow) previously unknown to the system is characterized based on the packet header information to determine the QoS requirements for the IP data flow, and to identify the subscriber CPE station that will receive the IP data flow.

During classification, the new IP data flow is classified into a communications priority class. Classification can also include grouping together packets from different IP flows having similar characteristics into a single class. Example class groupings of IP flows **630** are illustrated as IP classes **810***a*–**810***g*.

During presentation, the new IP data flow is initialized and presented to a downlink flow scheduler **604**.

Downlink flow scheduler places the data packets of an IP data flow into a class queue based on class queue priorities, and using a set of rules, schedules the data packets for transmission over a wireless medium to a subscriber CPE station **294** at subscriber CPE location **306** with an advanced reservation algorithm. The rules are determined by inputs to the downlink flow scheduler based on, e.g., a hierarchical class-based prioritization, a virtual private network (VPN) directory enabled data priority (such as, for example, directory enabled networking (DEN)), and a service level agreement priority. The advanced reservation algorithm for use in scheduling, e.g., isochronous traffic, is described with respect to FIG. **14** below.

SAR and framer **606** breaks up, sequences, and frames the data packets for wireless transmission from WAP **290***d* over the wireless medium to a wireless transceiver subscriber antenna **292**. Illustrated in block diagram **800** are a number of subscriber applications **820***a*–**820***e* running on devices such as, e.g., subscriber workstation **120***d* (not shown), connected to subscriber CPE stations **294***a*–*e* (not shown) located at subscriber CPE locations **306***a*–**306***e*. Each subscriber CPE location **306** can house one or more subscriber CPE stations **294**, and each subscriber CPE station **294** can receive and transmit one or more IP data flows to and from one or more subscriber workstations **120**. In fact, each application connected to a single CPE station can receive or transmit multiple IP data flows.

Referring to subscriber CPE location **306***a* of FIG. **8**A, a CPE SAR and framer **814***a* resequences the received data and transmits it through CPE flow scheduler **816***a*, and CPE IP flow analyzer **818***a*, to subscriber application **820***a*. CPE IP flow schedulers **816***a*–**816***e* can perform the same function as downlink flow scheduler **604** for uplink traffic. Similarly, CPE IP flow analyzers **818***a*–**818***e* perform the same function as downlink flow analyzer **602**.

In an embodiment of the invention, in downlink mode, CPE IP flow schedulers **816***a*–**816***e* and CPE IP flow analyzers **818***a*–**818***e* perform no function.

Block diagram **800** illustrates the logical functions performed on the downlink path, not necessarily the physical locations of these functions.

The functions of subscriber applications **820***a*–**820***e*, and CPE SAR and framers **814***a*–**814***e* can be performed in the actual subscriber CPE stations **294** connected over a wireless connection to wireless base station **302**.

Block diagram **800** lists an exemplary set of priorities **812** used by downlink flow scheduler **604** to place received data packets into priority class queues. Listed are the following set of example priorities: latency-sensitive UDP prority **812***a*, high priority **812***b*, intermediate priority **812***c*, initial hypertext transfer protocol (HTTP) screens priority **812***d*, latency-neutral priority **812***e*, file transfer protocol (FTP), simple mail transfer protocol (SMTP) and other e-mail traffic priority **812***f* and low priority **812***g*. Persons skilled in the art will recognize that many different priority classes are possible, depending upon the QoS requirements of the end-users. Latency-sensitive UDP priority data can refer to data that has the highest priority because it is sensitive to jitter (i.e., time synchronization is important) and latency (i.e., the amount of time passage between IP data flows in reverse directions). High priority **812***b* can refer to, e.g., premium VPN service, and a high priority SLA service. Intermediate priority **812***c* can refer to, e.g., a value VPN service level and an intermediate level SLA service. HTTP screens priority **812***d* can refer to the download of HTTP data, for example, an initial HTTP screen, which is important for making an Internet user feel as if he has a great deal of bandwidth available for his Internet session. Latency-neutral priority **812***e* can refer to data that is neutral to latency, such as, e.g., e-mail traffic. FTP, SMTP priority **812***f*

data includes data that is insensitive to latency and jitter, but requires a large amount of bandwidth to be downloaded accurately because of the size of a transmission. Finally, low priority data **812***g* can refer to data that can be transmitted over a long period of time, as when one network device transmits its status information to another network device on a 24 hour basis.

Block diagram **830** (of FIG. **8**B) depicts how IP flow analysis, prioritization and scheduling of the shared wireless bandwidth is performed in the uplink path, from subscriber CPE station **294***d*—to wireless transceiver subscriber antenna **292***d*—over the wireless medium—to WAP **290***d*—to wireless base station **302**—to interface **320**—to router **140***d*—to data network **140**.

Block diagram **830** includes uplink flow analyzer **632**, uplink flow scheduler **634** and uplink SAR and framer **636**. These components are similar in function to downlink flow analyzer **602**, downlink flow scheduler **604** and downlink SAR and framer **606**, but instead analyze, schedule and sequence and frame data packets being transmitted from subscriber workstations **120** of subscriber CPE stations **294** (at subscriber CPE locations **306***a*–**306***e*) over the wireless medium, and transmit the data packets to interface **320** for transmission to data network **142**.

Illustrated in FIG. **8**B are subscriber applications **820***a*–**820***e*, which are the same applications shown in FIG. **8**A. Also shown therein are CPE IP flow analyzers **819***a*–**819***e*, CPE IP flow schedulers **817***a*–**817***e*, and CPE SAR and framers **815***a*–**815***e*. These components function analogously to subscriber applications **820***a*–**820***e*, CPE IP flow analyzers **818***a*–**818***e*, CPE IP flow schedulers **816***a*–**816***e*, and CPE SAR and framers **814***a*–**814***e*. However, these components function to analyze, schedule and transmit IP flows in the uplink path, from subscriber CPE stations (at subscriber CPE locations **306***a*–**306***e*) to wireless base station **302** for routing to destination host workstations **136** (not shown).

As noted, multiple applications can be connected to one or more subscriber CPE stations at subscriber CPE locations **306***a*–**306***e*. To prevent collisions between multiple applications contending for a fixed number of bandwidth allocations for uplink communication, in one embodiment of the present invention a reservation scheduling system is used. The bandwidth allocations for data packets are called frame slots, and are described below with respect to FIGS. **12**A–**12**Q, **14**, **16**A and **16**B.

Block diagram **830** illustrates the logical functions performed on the uplink path, not necessarily the physical locations of these functions.

For example, in one embodiment, the analysis function of IP flow analyzer **632** which identifies a packet for uplink, characterizes and classifies the packet, can occur in a preferred embodiment in CPE IP flow analyzers **819***a*–**819***e* at the CPE subscriber stations **294***a*–**294***e* (not shown) at subscriber locations **306***a*–**306***e*.

Also, one embodiment, the functions of CPE IP flow schedulers **817***a*–**817***f* for scheduling uplinks subframe slots can be performed in wireless base station **302** for each of the subscriber CPE stations **294** connected over the wireless connection to wireless base station **302**.

In this embodiment, the scheduling function is performed at uplink flow scheduler **634** at wireless base station **302** based on classification information provided to the wireless base station **302** through an uplink IP flow reservation request from the CPE station. By placing all scheduling function at the wireless base station **302**, overall system quality of service can be optimized by centralizing the control of scheduling.

In another embodiment, however, their respective functions can be performed in the actual subscriber CPE stations.

In the reservation scheduling function of this embodiment, each subscriber CPE station requests the reservation of frame slots for its uplink transmissions using a reservation request block (RRB) of the TDMA airframe, described further below with reference to FIGS. **12**A–**12**O, before it is permitted to communicate in the uplink path with interface **320**. After the reservation request, uplink flow scheduler **634** transmits, as indicated by line **640**, to the requesting subscriber CPE station **294** a description of one or more slots which the CPE station **294** can use to transmit its uplink data packets from source subscriber workstations **120**, over the wireless medium, which are directed toward destination host workstations **136**, over data network **142**.

c. Service Level Requests

FIG. **9** illustrates how PRIMMA MAC IP flow scheduler **604** can also take into account a Service Level Agreement in prioritizing frame slot scheduling and resource allocation. FIG. **9** depicts SLA-mediated IP flow management diagram **900** including prioritization of uplink traffic being transmitted to wireless base station **302** from CPE subscriber locations **306***a*, **306***b*, **306***c* and **306***d*. For example, suppose subscribers of telecommunications services have subscribed to one of four SLA levels, P1 **902***a*, P2 **904***a*, P3 **906***a* and P4 **908***a*. In the illustrated example, suppose IP flows **902***b* are being sent to a subscriber at CPE location **306***a* and have an SLA priority level of P1 **902***a*. Similarly, IP flows **904***b*, **906***b* and **908***b* are being sent to subscribers at CPE locations **306***b*, **306***c* and **306***d* and have SLA priority levels of P2 **904***a*, **906***a* and **908***a*, respectively. PRIMMA MAC scheduler **604**, **634** of wireless base station **302** can take into account SLA-based priorities in allocating available bandwidth to the subscriber CPE IP flows **902***b*, **904***b*, **906***b* and **908***b*. In the example illustration, IP flow **902***b* can be allocated frame slot **902***c* based on SLA priority **902***a*. Frame slots **904***c*, **906***c* and **908***c* can be similarly scheduled taking into account SLA priorities. Uplinked IP flow traffic can then be transmitted on to data network **142**.

SLA-based prioritization can provide a valuable means for a telecommunications provider to provide differentiated services to a variety of customers. For example, it is possible that low priority traffic from a subscriber who has purchased a premium SLA service agreement, can be scheduled at a higher priority than high priority traffic from a subscriber which has only signed up for a value level or low cost SLA service priority.

d. Identification of Headers

FIG. **7** illustrates packet header field information **700** which can be used to identify IP flows and the QoS requirements of the IP flows. Specifically, IP header fields **702** can include, e.g., source and destination IP addresses, helpful in providing application aware preferential resource allocation; IP type of service (TOS), a useful field for assisting PRIMMA MAC in classifying a packet or IP flow; IP time to live (TTL), a useful field for anticipating application packet discards; and protocol fields which can be used in identifying IP flows.

Packet header information **700** also includes UDP header fields **704**. Included in UDP packet header fields **704** are source and destination port numbers.

Packet header information **700** also includes TCP header fields **706**. Included in TCP packet header fields **706** are source and destination port numbers; TCP sliding window size; urgent pointer; SYN, ISN, PSH, RST and FIN flags; and maximum segment size (MSS).

Packet header information **700** also includes realtime protocol RTP and RTCP header fields **708**.

It would be apparent to those skilled in the art that other packet header fields could be useful in identifying an IP flow. The fields have been given by way of example and are not intended to be an exhaustive list of useful packet header fields. Other fields, such as, e.g., fields from IP v6 relating to differentiated services (DIFF SERV) could also be useful to IP flow analyzer **602** and **632** of wireless base station **302**.

e. TDMA MAC Air Frame

FIGS. **12A–12O** illustrate an exemplary time domain multiple access (TDMA) media access control (MAC) transmission air frame. The fields described herein merely refer to one embodiment for the present invention, and are not limiting to the numerous implementations of the present invention.

FIG. **12A** illustrates an entire TDMA MAC transmission air frame. Air frame **1202** includes downstream transmission subframe **1202** and upstream transmission subframe **1204**.

The TDMA MAC air frame of FIG. **12A** includes upstream acknowledgment block (UAB) **1206**, acknowledgment request block (ARB) **1208**, frame descriptor block (FDB) **1210**, data slot $(DS)_1$ **1212***a*, DS_2 **1212***b*, DS_3 **1212***c*, DS_4 **1212***d*, DS_5 **1212***e*, DS_6 **1212***f*, DS_7 **1212***g*, DS_8 **1212***h*, DS_9 **1212***i*, DS_{10} **1212***j*, DS_{11} **1212***k*, DS_m **1212***l*, downstream acknowledgment block (DAB) **1214**, reservation request block (RRB) **1216**, UA_1 **1218***a*, UA_2 **1218***b*, UA_3 **1218***c*, UA_4 **1218U**, UA_5 **1218***e*, UA_6 **1218***f*, UA_7 **1218***g*, UA_8 **1218***h*, UA_9 **1218***i*, UA_{10} **1218***j*, UA_{11} **1218***k*, UA_{12} **1218***l*, and UA_n **1218***m*.

In the embodiment described herein, the type of TDMA used is TDMA/time division duplex (TDMA/TDD). In TDMA/TDD, for one interval of time, transmission is from a CPE station **294** to a wireless base station **302**, and in another instance of time, it is from a wireless base station **302** to a CPE station **194**. Any number of slots can be used for the uplink or for the downlink. The number of slots is dynamically assigned for both the uplink and the downlink. However, because the downlink data rate is usually higher than the uplink data rate, more slots are assigned to the downlink. Although distribution of slots between the downlink and uplink is dynamically assigned, the total number of slots for a frame is fixed in this embodiment.

TABLE 5

MAC Air Frame	Slots	Block/ SubFrame	Name	Description
0	1–8	DAB/ Upstream	Downstream Acknowledgment Request Block	Acknowledgments from subscribers CPE stations to wireless base station of receipt of downstream slots in previous downstream subframe
0	1–8	RRB/ Upstream	Reservation Request Block	Requests from subscriber CPE stations for transmission reservations in later frames with dynamically adjustable number of contentions slots
0	up to 16	US_1-US_{16}/ Upstream	Upstream Slot Transmissions	Data slots in the upstream subframe, which is a variable number per frame (up to 16 in one embodiment)

TABLE 5-continued

MAC Air Frame	Slots	Block/ SubFrame	Name	Description
0	1–3	ODB/ Upstream	Operations Data Block	OA&MP data from subscribers sequenced by a subscriber CPE station per frame
0	0	UAB/ Downstream	Upstream Acknowledgment Block	Acknowledgments from wireless base station to subscriber CPE stations of receipt of upstream slots in a previous subframe
0	0	ARB/ Downstream	Acknowledgment Request Block	Acknowledgments of subscriber CPE requests of having received reservation requests in a previous subframe
0	0	FD/ Downstream	Frame Descriptor Block for current frame	Describes the contents of the downstream transmission subframe
0	up to 16	DS_1-DS_{16}/ Downstream	Downstream Slot Transmission	Data slots in the downstream subframe, which is variable per frame (up to 16 in one embodiment)
0	0	CCB/ Downstream	Command and Control Block	OA&MP commands sequenced by subscribers per frame and frame synchronization

FIG. **12B** is a symbolic illustration of an exemplary TDMA/TDD air frame **1220** of the present invention. TDMA/TDD air frame structure **1220** depicts a frame of frame size **1228**, which can be, e.g., 16 slots or 32 slots. It would be apparent to those skilled in the art that frame structures **1220** having other numbers of slots could be used without departing from the spirit and scope of the invention. Frame structure **1220** includes, e.g., various TDMA slots **1222***a*, **1222***b*, **1222***c* and **1222***d*. Within each TDMA slot **1222***a–c*, can be included a data slot **1224***a*, **1224***b*, **1224***c* and **1224***d* which in turn can contain a control packet **1226***a*, or a data packet **1226***b–d*, respectively.

In the present embodiment the sum of all TDMA slots **1222** within a frame of frame size **1228** is fixed. However, as noted, using the resource allocation methodologies of the present invention it is possible to dynamically allocate a subset of the entire number of TDMA slots **1222** to an uplink direction, where all the uplink TDMA slots are known collectively as an uplink subframe or an upstream transmission subframe **1204**, and to dynamically allocate a subset of the entire number of TDMA slots **1222** to a downlink direction, where all the downlink TDMA slots are known collectively as a downlink subframe or an downlink transmission subframe **1202**. Using the resource allocation method of the present invention, it is possible to allocate all TDMA slots **1222** to a given upstream or downstream direction. It is further possible to allocate all data slots **1224** to a single CPE station. The wireless base station **302** has a state machine, and knows the state of each CPE station **294** having a connection therewith (i.e., having an IP flow recognized by the wireless base station **294**).

Downstream transmission subframe **1202** and upstream transmission subframe **1204** are described in detail below.

1. Downstream Transmission Subframe

FIG. **12C** depicts an exemplary downstream transmission subframe **1202**. The downstream transmission subframe of

FIG. 12C includes transmitter turnaround time **1230**, UAB **1206**, ARB **1208**, FDB **1210**, a variable number of DSs per frame (e.g., 16) **1212**, and command and control block (CCB) **1232**. The DS transmissions **1212** include DS_1 **1212***a*, DS_2 **1212***b*, DS_3 **1212***c*, DS_4 **1212***d*, DS_5 **1212***e*, DS_6 **1212***f*, $DS_{7\ 1212}$*g*, DS_8 **1212***h*, DS_9 **1212***i*, DS_{10} **1212***j*, DS_{11} **1212***k*, and DS_m **1212***l*.

FIG. 12D depicts an exemplary UAB **1206** of a downstream transmission subframe **1202**. The downstream transmission subframe of FIG. 12D includes UAB **1206**, ARB **1208**, FDB **1210**, DS_1 **1212***a*, DS_2 **1212***b*, DS_3 **1212***c*, DS_4 **1212***d*, DS_5 **1212***e*, DS_6 **1212***f*, DS_7 **1212***g*, DS_n **1212***h*, DS_9 **1212***i*, DS_{10} **1212***j*, DS_{11} **1212***k*, DS_m **1212***l*, and CCB **1232**.

UAB **1206** includes subslots UAB_1 **1206***a*, UAB_2 **1206***b*, UAB_3 **1206***c*, UAB_4 **1206***d*, UAB_5 **1206***e*, UAB_6 **1206***f*, UAB_7 **1206***g*, and UAB_n **1206***h*. UAB_1 **1206***a* includes a preamble **1234***a*, subscriber ID **1234***b*, IP-flow identifier **1234***c*, slot sequence number **1234***d*, and cyclical redundancy check (CRC) **1234***e*.

The UAB field is an acknowledgment by a wireless base station **302** to a CPE station **294** that the slots (e.g., US_1–US_{16}) of an upstream transmission subframe have been received. The reader is referred to the discussion of the upstream transmission subframe below.

In subslot UAB_1 **1206***a* of ARB **1206**: preamble **1234***a* includes data used for link integrity purposes; subscriber ID **1234***b* identifies which CPE station **294** is making the reservation request; IP-flow identifier **1234***c* identifies the IP data flow; quality of service data class **1234***a* identifies the priority class of the IP data flow, if known to the CPE station **294**; IP-flow priority and type **1234***b* is an indicator of a new IP data flow; and CRC **1234***e*, which stands for cyclic redundancy code, provides error checking bits for subslot RRB_1 **1216***a*.

FIG. 12E depicts an exemplary ARB **1208** of a downstream transmission subframe **1202**. The downstream transmission subframe of FIG. 12E includes UAB **1206**, ARB **1208**, FDB **1210**, DS_1 **1212***a*, DS_2 **1212***b*, DS_3 **1212***c*, DS_4 **1212***d*, DS_5 **1212***e*, DS_6 **1212***f*, DS_7 **1212***g*, DS_n **1212***h*, DS_9 **1212***i*, DS_{10} **1212***j*, DS_{11} **1212***k*, DS_m **1212***l*, and CCB **1232**.

ARB **1208** includes subslots ARB_1 **1208***a*, ARB_2 **1208***b*, ARB_3 **1208***c*, ARB_4 **1208***d*, ARB_5 **1208***e*, ARB_6 **1208***f*, ARB_7 **1208***g*, and ARB_n **1208***h*. ARB_1 **1208***a* includes a preamble **1234***a*, subscriber ID **1234***b*, IP-flow identifier **1234***c*, slot sequence number **1234***d*, and CRC **1234***e*.

The ARB field is an acknowledgment by a wireless base station **302** to a CPE station **294** that the wireless base station **302** has received an upstream reservation request from the CPE station **294**. The reader is referred to the discussion of the upstream transmission subframe below.

In subslot ARB_1 **1208***a* of ARB **1208**: preamble **1234***a* includes data used for link integrity purposes; subscriber ID **1234***b* identifies which CPE station **294** is making the reservation request; IP-flow identifier **1234***c* identifies the IP data flow;quality of service data class **1234***a* identifies the priority class of the IP data flow, if known to the CPE station **294**; IP-flow priority and type **1234***b* is an indicator of a new IP data flow; and CRC **1234***e*, which stands for cyclic redundancy code, provides error checking bits for subslot RRB_1 **1216***a*.

FIG. 12F depicts an exemplary FDB **1210** of a downstream transmission subframe **1202**. The downstream transmission subframe of FIG. 12F includes UAB **1206**, ARB **1208**, FDB **1210**, DS_1 **1212***a*, DS_2 **1212***b*, DS_3 **1212***c*, DS_4 **1212***d*, DS_5 **1212***e*, DS_6 **1212***f*, DS_7 **1212***g*, DS_n **1212***h*, DS_9 **1212***i*, DS_{10} **1212***j*, DS_{11} **1212***k*, DS_m **1212***l*, and CCB **1232**.

The FDB includes detailed information pertaining to the slots (e.g., DS_2–DS_{16}) of the downstream transmission subframe.

FDB **1210** includes a preamble subslot **1236***a*, number of downstream slots subslot, **1236***b*, IP-flow ID for upstream reservation 1 subslot **1236***c*, IP-flow ID for upstream reservation 2 subslot **1236***d*, IP-flow ID for upstream reservation n subslot **1236***e*, and contention slot count for next upstream subframe subslot **1236***f*.

In FDB **1210**, the fields are defined as follows: preamble subslot **1236***a* includes data used for link integrity purposes; number of downstream slots subslot **1236***b* includes the number of downstream slots (DSs), IP-flow ID for downstream reservation subslot **1236***c* includes an IP flow identification for DS_1; IP-flow ID for downstream reservation subslot **1236***d* includes a second IP flow identification for DS_2; IP-flow ID for downstream reservation n subslot **1236***e* includes another IP flow identification for DS_m; contention slot count for next upstream subframe subslot **1236***f* provides a count for the next available upstream subframe.

FIG. 12G depicts an exemplary downstream MAC payload data unit (PDU). The downstream MAC PDU includes information regarding the actual structure of the payload. The downstream MAC PDU of FIG. 12G includes MAC linked list sequence number **1238***a* (the sequence number of the MAC linked list), reservation request index number **1238***b* (an index to the downstream IP flow), compressed IP-flow identifier **1238***c*, compressed IP-flow priority and type **1238***d* (identifying the priority and type of a compressed IP flow), slot payload **1238***e* (the amount of data in a downstream data slot), and CRC **1234***e* (error checking information).

FIG. 12H depicts an exemplary CCB of a downstream transmission subframe **1202**. The CCB comprises OAM&P commands sequenced by subscriber CPE station **294** per frame and frame synchronization. CCB **1232** includes a mode command subslot **1240***a* (includes options of what mode the CPE station is to take), profile command subslot **1240***b* (includes specific system commands, such as a patch for a module), control data index subslot **1240***c* (including download-locations and-memory-requirements or other information needed by the CPE stations to download data), datablock 1 subslot **1240***d* (includes specific system data), datablock 2 subslot **1240***e* (same), datablock n subslot **1240***f* (same), and CRC subslot **1234***e* (error checking information).

2. Upstream Transmission Subframe

FIG. 12I depicts an exemplary upstream transmission subframe **1204**. The upstream transmission subframe of FIG. 12I includes transmitter turnaround time **1230**, DAB **1214**, RRB **1216**, a variable number of USs per frame, e.g., 16, **1218**, and operations data block (ODB) **1242**, consisting of OAM&P data from subscribers, sequenced by subscriber per frame. The US transmissions **1218** include US_1 **1218***a*, US_2 **1218***b*, US_3 **1218***c*, US_4 **1218***d*, US_5 **1218***e*, US_6 **1218***f*, US_7 **1218***g*, US_8 **1218***h*, US_9 **1218***i*, US_{10} **1218***j*, US_{11} **1218***k*, $US_{12\ 1218}$*l*, and US_n **1218***m*.

FIG. 12K depicts an exemplary RRB **1216** of an upstream transmission subframe **1204**. The upstream transmission subframe of FIG. 12K also shows DAB **1214**, RRB **1216**, US_1 **1218***a*, US_2 **1218***b*, US_3 **1218***c*, US_4 **1218***d*, US_5 **1218***e*, US_6 **1218***f*, US_7 **1218***g*, US_8 **1218***h*, US_9 **1218***i*, US_{10} **1218***j*, US_{11} **1218***k*, US_{12} **1218***l*, US_n **1218***m*, and ODB **1242**.

RRB **1216** includes subslots RRB_1 **1216***a*, RRB_2 **1216***b*, RRB_3 **1216***c*, RRB_4 **1216***d*, RRB_5 **1216***e*, RRB_6 **1216***f*, RRB_7 **1216***g*, and RRB_n **1216***h*. RRB_1 **1216***a* includes a preamble **1234***a*, subscriber ID **1234***b*, IP-flow identifier **1234***c*, quality of service data class **1244***a*, IP-flow priority and type **1244***b*, and CRC **1234***e*.

A CPE station **294** uses one of the subslots (RRB_1 **1216***a*, RRB_2 **1216***b*, RRB_3 **1216***c*, RRB_4 **1216***d*, RRB_5 **1216***e*,

RRB_6 **1216***f*, RRB_7 **1216***g*, and RRB_n **1216***h*) of RRB **1216** to make a reservation request, which is a request by the CPE station **294** for bandwidth in a future uplink transmission subframe. If two CPE stations **294***d*, **294***e* attempt to access the same subslot in RRB **1216**, which can occur because their pseudorandom number generators select the same subslot, then a "collision" occurs and the data is not readable by wireless base station **302**. The two CPE stations **294***d*, **294***e* are required to try again.

Reservation request slots can be provided on an IP flow basis. Rather than allocate a reservation request slot to every CPE subscriber station, a default number (e.g., 5) are made available as contention slots. If collisions are detected by a greater number of requesting subscribers than the number of reservation request slots, then the slots allocated can be dynamically varied to provide additional RRB slots. (Collisions are analogous to CSMA/CD collisions in Ethernet, where colliding devices on an Ethernet network attempt to retransmit over the bus architecture by retrying at a random time.)

The radio contention method of the present invention builds upon aspects of the "Slotted Aloha" method developed by L. Roberts in 1972, as a refinement of the "Aloha" method developed by N. Abramson in the early 1970's, and so-called bit-mapped reservation protocols. Like the Slotted Aloha method, the present invention provides for discrete slots for transmission of data, rather than allowing the transmission of data at any point. However, instead of transmitting the actual "payload" of data, the present invention advantageously transmits only a "reservation request" describing the actual data payload contents. Also, the number of slots for reservation requests can advantageously be dynamically altered according to the frequency of detected collisions in the recent past.

Unlike various Carrier Sense Multiple Access (CSMA) techniques previously used in wireless, both persistent and non-persistent, the present method advantageously does not require that subscriber CPE station **294***d* "sense" the carrier (the radio channel) before transmission. Instead, a subscriber CPE station **294***d* selects a "subslot" to transmit through a pseudo-random number selection, without a prior carrier sense. If a collision is detected, the subscriber CPE station **294***d* will try again in the next frame using the pseudo-random number process.

Instead of using a bit-map protocol for the resolution of contention, as is used in some reservation protocols, the wireless base station can explicitly grant reservation requests. The standard bit-map protocol can require that all stations can receive signals from all other stations so that the subsequent order of transmission can be implicitly determined from the resulting bit-map pattern. The present method advantageously does not require the receipt of reservation request signals from other CPE subscriber stations **294***d*. This is advantageous because, at higher frequencies (such as, e.g., 2 GHz to 30 GHz) where there may be line-of-sight and distance constraints, the requirement for receipt of the transmissions of other CPE subscriber stations **294***d* could unduly constrain the topology, locations and distances of CPE subscriber stations.

Advantageously, by allowing the wireless base station **302** to explicitly grant the requested reservation, other factors such as relative or dynamic CPE subscriber station **294***d* (or IP-flow) priority factors can be considered. Therefore, the present invention's reservation protocol with a dynamically adjustable number of contention subslots and explicit wireless base station reservation grants, allows a more optimal means of providing for the allocation of wireless, such as, e.g., radio, bandwidth in response to QoS requirements of IP-flows than any prior method.

As noted, RRB_1 **1216***a* includes the following fields: a preamble **1234***a*, subscriber ID **1234***b*, IP-flow identifier **1234***c*, quality of service data class **1244***a*, IP-flow priority and type **1244***b*, and CRC **1234***e*. In subslot RRB_1 **1216***a* of RRB **1216**: preamble **1234***a* includes data used for link integrity purposes; subscriber ID **1234***b* identifies which CPE station **294** is making the reservation request; IP-flow identifier **1234***c* identifies the IP data flow;quality of service data class **1234***a* identifies the priority class of the IP data flow, if known to the CPE station **294**; IP-flow priority and type **1234***b* is an indicator of a new IP data flow; and CRC **1234***e*, which stands for cyclic redundancy code, provides error checking bits for subslot RRB_1 **1216***a*. Optionally, an additional field can be provided in subslot RRB_1 **1216***a* which includes the number of data packets CPE station **294** will transmit in its IP data flow.

FIG. **12**J depicts an exemplary DAB **1214** of an upstream transmission subframe **1204**, where a CPE acknowledges receipt of a slot from base. The DAB is an acknowledgment from a subscriber CPE station **294** to the wireless base station that downstream slots have been received in a previous subframe.

The DAB **1214** includes subslots DAB_1 **1214***a*, DAB_2 **1214***b*, DAB_3 **1214***c*, DAB_4 **1214***d*, DAB_5 **1214***e*, DAB_6 **1214***f*, DAB_7 **1214***g*, and DAB_n **1214***h*. Subslot DAB_1 **1214***a* includes a preamble **1234***a*, subscriber ID **1234***b*, IP-flow identifier **1234***c*, slot sequence number **1234***d*, and CRC **1234***e*. (These fields have the same information as described with respect to the RRB.)

FIG. **12**L depicts an exemplary MAC PDU upstream slot. The MAC PDU upstream slot of FIG. **12**L includes a CPE linked-list sequence number **1246**, reservation request index number **1236***b*, compressed IP-flow identifier **1238***c*, compressed IP-flow priority and type **1238***d*, slot payload **1238***e*, and CRC **1234***e*. The upstream MAC PDU is similar to the downstream-MAC PDU, but is-used instead for upstream subframe payload information.

FIGS. **12**M, **12**N and **12**O depict an exemplary ODB **1242** in detail. This field is used to store information regarding the connection between the wireless base station **302** and the CPE station **294**. ODB **1242** includes preamble **1234***a* (including link integrity data), subscriber ID **1234***b* (identifies which CPE station **294** is making the reservation request), system state **1248***a* (information about the status of the CPE station **294**), performance data **1248***b* (how full the buffer statistics, cpe processor performance statistics, system state), antenna data **1248***c* (information pertaining to the antenna), CRC **1234***e* (error checking information) and synchronization pattern **1248***d* (error checking information).

Referring to FIG. **12**M, system state subslot **1248***a* comprises system mode **1250***a* (the mode of the CPE station, e.g., command mode, operations mode, or initialization mode of the system), system status **1250***b* (the status of the CPE station), system resources **1250***a* (the mode of the CPE station), system power **1250***b* (the mode of the CPE station), system temperature **1250***a* (the temperature of the CPE station). The CPE stations **294** are required to take turns using ODB **1242** to transmit their information.

Referring to FIG. **12**N, performance data **1248***a* comprises the number of comrepeats **1252***a* (the number of repeats of communication attempts), number of frameslips **1252***b* (the number of frames that have slipped), waitstate index **1252***c* (an index to the waiting state).

f. Exemplary Class-based Frame Prioritization

FIG. **13** shows block diagram **1300**, illustrating how an exemplary flow scheduler for the present invention functions

to schedule products. Block diagram **1300** includes: flow scheduler **604**, **634** (which is a combination of downlink flow scheduler **604** and uplink flow scheduler **634**), downlink transmission subframe **1202** (i.e., the next MAC downstream subframe), uplink transmission subframe **1204** (i.e., the current MAC upstream subframe). Block diagram **1300** also includes the following downstream components: downstream reservation first-in-first-out queue **1322**, class 1 downstream queue **1302**, class 2 downstream queue **1304**, and class 3 downstream queue **1306**. Block diagram **1300** also includes the following upstream reservation components: current upstream subframe **1344** (with the current upstream subframe **1204** about to be stored in it), previous upstream subframes **1346**, **1348**, **1350**, class 1 upstream reservation request queue **1308**, class 2 upstream reservation request queue **1310**, and class 3 upstream reservation request queue **1312**.

In the downlink path, an IP flow QoS class queuing processor (described below with respect to FIGS. **15**A and **15**B) queues the received data packets into class 1 packet flow queues **1324**, **1326** and **1328**, class 2 packet flow queues **1330**, **1332**, **1334**, and class 3 packet flow queues **1336**, **1338**, **1340** and **1342**.

Based on inputs from a hierarchical class-based priority processor, a virtual private network (VPN) directory enabled (DEN) data table and a service level agreement (SLA) priority data table (described below with respect to FIGS. **15**A and **15**B), the class 1, class 2, and class 3 packet flow queues are respectively assigned to class 1 downstream queue **1302**, class 2 downstream queue **1304**, and class 3 downstream queue **1306**. Flow scheduler **604**, **634** schedules these downlink data packets onto the downlink transmission subframe **1202**.

In one embodiment, additional processing is used to minimize latency and jitter. For example, suppose the data packets of class 1 packet flow queue **1324** require jitter-free and latency-free delivery, i.e., delivery of packets must be at constant time intervals and in real-time. Packet flow queue **1324** creates, e.g., 4 equal time spaced slot reservations in future frames, as shown in class 1 downstream queue **1302** and described with respect to FIG. **14** below. The reservations are fed to downstream reservation first-in-first-out queue **1322**, and are scheduled onto a future downstream frame **1202** by flow scheduler **604**, **634**.

In the uplink path, reservation requests for future upstream slots arrive at wireless base station **302** as part of the current upstream subframe **1204** received from CPE subscriber stations **294** over the wireless medium. Current upstream subframe **1344** can temporarily store reservation requests for analysis and scheduling of uplink packets in accord with the description of FIG. **8**B above. Previous upstream subframes **1346**, **1348**, **1350** include upstream reservation requests awaiting upstream frame slot allocations in future upstream subframes **1204**. Reservation request blocks (RRBs), described further above with reference to FIG. **12** * * *, include a request for a number of slots for a single IP flow with an IP flow identifier # and class of the flow. The upstream reservation requests (by IP flow and class) are queued onto class 1 upstream reservation request queue **1308**, class 2 upstream reservation request queue **1310**, and class 3 upstream reservation request queue **1312** by an IP flow QoS class queuing processor (described below with respect to FIGS. **16**A and **16**B). Flow scheduler **604** and **1566**, and **634** and **1666**, uses these downstream reservations and upstream reservation requests to assign slots to data packets in the next downstream transmission subframe **1202** and upstream transmission subframe **1204**, respectively.

FIG. **14** is an exemplary two-dimensional block diagram **1400** of the advanced reservation algorithm. FIG. **14** includes MAC subframe scheduler **1566**, **1666**, frames current frame, n **1402**, and future frames, n+1 1404, n+2 **1406**, n+3 **1408**, n+4 **1410**, n+5 **1412**, n+6 **1414** . . . n+x **1416**, representing frames of data packets to be transmitted at times n, n+1, n+2 . . . n+x. Each frame is divided into a variable length downlink subframe **1202** and a variable length uplink subframe **1204**. The lengths of downlink subframe **1202** and uplink subframe **1204** together comprise the length of an entire frame.

Each frame n **1402** includes a number of slots (**1418**–**1478**). Slots **1418**–**1446** comprise the downlink subframe **1202**, and slots **1448**–**1478** comprise the uplink subframe **1204**. In one embodiment, the slots are fixed in length, with each slot capable of storing a single data packet. The total number of frame slots in a frame remains constant. For example, if a given frame includes 64 frame slots, the slots can be allocated dynamically in either the uplink or downlink directions, such as, e.g., 32 up and 32 down, 64 up and 0 down, 0 up and 64 down. Block diagram **1400** can be thought of as a two dimensional matrix with each slot having a time value (i.e., a slot-to-slot time interval), e.g., 0.01 ms, and each frame having a total frame interval time value (i.e., a frame-to-frame time interval), e.g., 0.5 ms.

In the present invention, an advanced reservation algorithm assigns future slots to data packets based on the priority of the IP data flow with which the packet is associated. Exemplary priorities are described above with respect to FIGS. **8**A and **8**B. For calls that are sensitive to jitter, meaning calls that are time sensitive, it is important to maintain an isochronous (i.e., in phase with respect to time) connection. With such signals, it is important that the data be dispersed in the same slot between frames, or in slots having a periodic variation between frames. For example, vertical reservation **1480** shows a jitter sensitive signal receiving the same slot-for-downlink communications in each frame. Specifically, the signal is assigned slot **1422** in frames **1402**–**1416**. If the frame-to-frame interval is 0.5 ms, then a slot will be provided to the IP flow every 0.5 ms. As another example, diagonal reservation **1482** shows a jitter sensitive signal receiving a slot varying by a period of one between sequential frames. Specifically, the signal is assigned slot **1440** in frame **1402**, slot **1438** in slot **1404**, . . . slot **1426** in frame **1416**, to create a "diagonal." If the frame-to-frame interval is 0.5 ms and the slot-to-slot interval is 0.01 ms, then a slot can be provided to the IP flow every 0.5 minus 0.01, equals 0.49 mms. Thus, to decrease the frame interval, a diagonal reservation of positive slope can be used. To obtain an increased frame interval, a diagonal of negative slope such as, e.g., negative slope diagonal uplink reservation **1486**. The diagonal reservation **1482** can also be more pronounced (i.e., using a greater or lesser slope), depending on the period between sequential frames desired. Reservation patterns **1480**, **1482**, **1484** and **1486** are useful patterns for jitter sensitive communications. Also illustrated is a vertical reservation **1486**, similar to vertical reservation **1480**, useful for a jitter sensitive communication in the uplink direction.

For latency sensitivity, one or more slots can be guaranteed in each frame. For example, for a call that is latency sensitive, but not jitter sensitive, each frame can be assigned one (or more) slots for communications. However, the slot(s) need not be periodic between frames, as with jitter sensitive calls. The greater the number of slots allocated per frame to an IP flow, the greater total bandwidth per frame rate for the IP flow.

For calls that are less latency sensitive, fewer slots per frame can be assigned for the communication. For example, a communication that is less latency sensitive can receive a guaranteed bandwidth of one slot every four frames. A call that is even less latency sensitive can receive, e.g., a single slot every ten frames.

Using these principles, the advanced reservation algorithm can assign the slots from highest priority to lowest priority, exhausting the number of available slots in future frames. IP data flows that are both jitter and latency sensitive can be assigned slots with periodic patterns first (e.g., patterns **1480**, **1482**, **1484** and **1486**), followed by flows that are highly latency sensitive (but not jitter sensitive), et cetera, until the flows of lowest latency sensitivity are assigned to slots. Prioritization of different classes of IP flows by scheduler **604**, **634**, **1566**, **1666** is described further below with reference to FIGS. **15**A, **15**B, **16**A and **16**B.

g. Downlink SubFrame Prioritization

1. Overview

FIGS. **15**A and **15**B are exemplary logical flow diagrams for analysis and scheduling of the shared wireless bandwidth for the downlink direction. The logical flow pertains to IP packet flows arriving from data network **140**, at the wireless base station **302**, for transmission down to a subscriber CPE station **294***d* over the wireless medium. FIG. **15**A is an exemplary logical flow diagram **1500** for downlink IP analyzer **602**. FIG. **15**B is an exemplary logical flow diagram **1560** for the downlink flow scheduler **604**.

The functional components for FIGS. **15**A and **15**B are explained by way of method modules, which can be viewed as physical units (e.g., comprising software, hardware, or a combination thereof) or logical vehicles (e.g., used for explanatory purposes only). Those skilled in the art will recognize that the modules are used only to explain an exemplary embodiment, and are not to be considered limiting.

The exemplary logical flow diagram **1500** for downlink IP flow analyzer of FIG. **15**A includes packet header identification component **1502**, packet characterization component **1504**, packet classification component **1506**, and IP flow presentation component **1508**. The functions of these components are explained in detail below.

In one embodiment, downlink IP flow analyzer **602** is physically located in wireless base station **302**, although those skilled in the art will recognize that the same functionality can be located remotely from wireless base station **302**.

FIGS. **2**D, **3**A and **3**B are helpful to the reader for an understanding of the downlink IP flow analyzer.

2. Introduction

IP flow analyzer **602** performs the function of identifying, characterizing, classifying, and presenting data packets to a downlink frame scheduler **604**. The functions of identifying, characterizing, classifying and presenting the data packets are respectively performed by packet header identification component **1502**, packet characterization component **1504**, packet classification component **1506** and IP flow presentation component **1508** of downlink IP flow analyzer **602**.

Packet header identification component **1502** determines whether a data packet of an incoming IP data flow is part of an IP flow that is known to the system, or is the first data packet of a new IP data flow, based on the contents of fields of the packet header section. Packet header identification component **1502** also identifies, e.g., the source of the packet using the packet header field contents. Packet characterization component **1504** characterizes a new data packet (of a new IP data flow) to determine the QoS requirements for the IP data flow, and identifies the subscriber CPE station associated with the subscriber workstation that will receive the IP data flow. Packet classification component **1506** classifies the new IP data flow into a communications priority class, grouping the packet together with similar type IP flows. IP data flow presentation **1508** initializes the new IP data flow and presents it to downlink flow scheduler **604**.

Downlink flow scheduler **604** places the data packets of an IP data flow into a class queue, and based on a set of rules, schedules the data packets for transmission over the wireless medium to a subscriber CPE station using, e.g., an advanced reservation algorithm. The rules can be determined by inputs to the downlink flow scheduler from a hierarchical class-based priority processor module **1574**, a virtual private network (VPN) directory enabled (DEN) data table **1572**, and a service level agreement (SLA) priority data table **1570**. The advanced reservation algorithm is described further above with respect to FIG. **14**.

3. Identification

Packet header identification component **1502** identifies the IP flow received from data network **142** at data interface **320** based on the packet header.

An IP flow packet stream from data network **142**, including packets from various IP flows (where each IP flow is associated with a single data "call") is received at packet header identification component **1502**. An IP flow can include packetized data including any type of digital information such as, e.g., packetized voice, video, audio, data, IP flows, VPN flows, and real time flows. The IP flow is transmitted over data network **142** from, e.g., a host workstation **136***d* and arrives at interface **302** of wireless base station **320**. Interface **302** transmits the packets of the IP flow to packet header identification component **1502**. At module **1510**, the received packets are buffered into a storage area. At module **1520**, the contents of the packet header fields are extracted and parsed.

For IP flows known to the system, so-called "existing IP flows," there are entries in a table **1526**. An IP flow is in the system if there is an existing characterized IP data call. In module **1522**, it is determined if there is a match between the incoming packet and an existing IP flow call in an entry in existing IP flow identification table **1526**. If so, then the IP flow is known to the system, and control passes to module **1530** of the packet characterization component **1504**.

If not, meaning that the IP flow is a new IP data flow, then control passes to module **1524**, where the packet header fields are analyzed. Module **1524** analyzes the packet header source field and determines from source application packet header data table **1528** the type of source application making the data call or transmitting the IP packet. The application can be any of the applications described with respect to FIG. **2**D or known to those skilled in the art. Examples include a file transfer protocol (FTP) download from another client workstation **138***f*, an IP voice telephony call (over telephony gateway **288***b*), a voice telephony call from a caller **124***d* (connected over a modem), an e-mail from a LAN **128***a* attached host workstation **136***a*, a fax machine call, and a conference call from multiple callers **124***d* and **126***d* (connected over a modem), to name a few. If the IP flow is not known to the system, then the IP flow is given an IP flow identifier number, and control passes to module **1526** where the IP flow identifier number is added to the existing IP flow identification table **1526**.

Once the type source application has been determined by packet header information or by another means, such as direct application identification, then control passes from module **1524** to module **1532** of the packet characterization

component **1504**. In order to identify the type of source application of the IP flow, any type of service (TOS) or differentiated service (DiffServ) field can also be analyzed.

4. Characterization

Packet characterization component **1504** characterizes new IP flows and passes them to packet classification component **1506** for classification.

For an existing IP flow, control passes to module **1530** from module **1522** of the packet header identification component **1502**. If in module **1522** it is determined that the IP data flow is known to the system, in module **1530** it is determined whether the packet is old (i.e., stale). This can include, e.g., determining from a time-to-live field (a field in the IP packet header) the age of the packet, and comparing the field to a threshold age value. If the packet is determined to be stale, it can be discarded. Based on the age of the packet, client application discards can be anticipated. Otherwise, control can pass to module **1540** of the packet classification component **1506**.

For a new IP flow, control passes to module **1532** from module **1524** of the packet header identification component **1502**. If in module **1524** it is determined that the IP flow is not known to the system, in module **1532** the QoS requirements for the application are determined using the source application information identified in modules **1524** and **1528**. Module **1532** performs this operation by looking up the QoS requirements for the identified source application in the QoS requirement table **1534**. Different applications have different QoS requirements in order to provide an acceptable end-user experience. For example, bandwidth allocation (i.e., allocating an appropriate amount of bandwidth) is important to an application performing FTP file transfer downloads, and not jitter (i.e., time synchronizing the received data) and latency (i.e., the amount of time passage between responses). On the other hand, jitter and latency are important to voice telephony and conference calls, while bandwidth allocation is not.

After processing by module **1532**, in module **1536** a destination CPE subscriber station ID lookup from subscriber CPE IP address table **1538**, is performed for the IP flow. Each subscriber CPE station **294***d* can have one or more applications, running on one or more subscriber workstations **120***d*, homed to it. Accordingly, the IP flows can be directed to one or more applications on one or more subscriber workstations of one or more CPE stations **294***d*. A subscriber workstation can be any device coupled to a subscriber CPE station **294***d*. Module **1536** looks up the IP flow in table **1538**, to determine the identity of the subscriber CPE station **294***d* that will receive the packets of the new IP flow from data network **142**. Control then passes from module **1536** to module **1542** of the packet classification component **1506**.

5. Classification

Packet classification component **1506** classifies the IP flow and passes it to IP flow presentation component **1508** for presentment.

For an existing IP flow, control passes to module **1540** from module **1530** of the packet characterization component **1504**. If in module **1530** it is determined that the packet is not stale, then in module **1540** the packet is associated with its existing IP flow. As illustrated in FIG. **15A**, the packet processed herein was determined to be a portion of an IP flow known to the system. Therefore, the QoS processing of modules **1532**, **1536** and **1542** are unnecessary, because the QoS requirements of the present packet are assumed to be the same as for its IP flow. In another embodiment, all packets are characterized and classified. From module **1540**, control can continue with module **1546** of IP flow presentation **1508**.

For the new IP flow, control passes to module **1542** from module **1536** of the packet characterization component **1504**. In module **1542** the packet is classified into a QoS class by performing a table lookup into IP flow QoS class table module **1544**, where the types of QoS classes are stored depending on the QoS requirements for packets. Similar IP flows, (i.e., IP flows having similar QoS requirements) can be grouped together in module **1542**. In classifying packets and IP flows, QoS class groupings, any DiffServ priority markings, and any TOS priority markings can be taken into account. From the module **1542**, control passes to module **1548** of IP flow presentation component **1508**.

6. IP Flow Presentation

IP flow presentation component **1508** prepares and presents the IP flow packets to downlink flow scheduler **604**.

For existing IP flows, control passes to module **1546** from module **1540** of the packet classification component **1540**. In module **1546** the packet is added to the associated existing IP flow queue, which is the queue for the current IP flow. From module **1546**, control passes to IP flow QoS class queuing processor module **1562** of downlink flow scheduler **604**.

For the new IP flow, control passes to module **1548** from module **1542** of the packet classification component **1506**. In module **1548**, this new IP flow can be initialized for presentation to module **1552**. In module **1550**, the IP flow QoS class is presented to frame scheduler **604** to be placed in an appropriate class queue. Module **1552** presents the IP flow (in particular, the data packet) and IP flow identifier to IP flow QoS class queuing processor module **1562** of downlink flow scheduler **604**.

7. Downlink Flow Scheduler

The exemplary logical flow diagram **1560** for the downlink flow scheduler **604** of FIG. **15B** comprises IP flow QoS class queuing processor module **1562**, MAC downlink subframe scheduler module **1566**, hierarchical class-based priority processor module **1574**, VPN DEN data table module **1572**, SLA priority data table **1570**, CPE IP flow queue depth status processor **1582** and link layer acknowledgment processor module **1578**.

Downlink flow scheduler **604** of FIG. **15B** also includes QoS class queues as follows: class 1, **1564***a*; class 2, **1564***b*; class 3, **1564***c*; class 4, **1564***d*; class 5, **1564***e*; and class 6, **1564***f*; and MAC downlink subframes: frame n, **1568***a*; frame n+1, **1568***b*; frame n+2, **1568***c*; frame n+3, **1568***d*; . . . frame n+p, **1568***k*.

In one embodiment, downlink flow scheduler **604** is physically located in wireless base station **302**, although those skilled in the art will recognize that the same functionality can be located remotely from wireless base station **302**.

Downlink flow scheduler **604** is used to schedule the downlink subframe. An entire frame can be divided into an uplink portion (called an uplink subframe) for transmitting uplink frames, and a downlink portion (called a downlink subframe) for transmitting downlink frames.

Also illustrated on FIG. **15B** are WAP antenna, the wireless medium, **290***d*, RF transceiver subscriber antenna **292***d*, subscriber CPE station **294***d* and subscriber workstation **120***d*. WAP antenna **290***d* and RF transceiver subscriber antenna **292***d* respectively provide a wireless connection between wireless base station **302** (where downlink flow scheduler **604** resides in one embodiment) and subscriber CPE station **294***d*, which can transmit an IP flow to an application running on subscriber workstation **120***d*. WAP antenna **290***d* serves as a wireless gateway for data network

142, and RF transceiver subscriber antenna serves as a wireless gateway for subscriber CPE station **294***d*. The connection is also illustrated in FIGS. **2**D and **3**B.

IP flow QoS class queuing processor module **1562** receives the packets from IP flow presentation component **1508**. Module **1562** then creates class queues **1564***a*–**1564***f*, which is a variable number of queues, and places the packets in these class queues. How packets are placed in class queues **1564***a*–**1564***f* is determined by the inputs to module **1562**.

Module **1562** can receive inputs from hierarchical class-based priority processor module **1574**, VPN DEN data table **1572** and service level agreement (SLA) priority data table **1570**. The queuing function of module **1562** can be based on these inputs.

SLA priority data table **1570** can use predetermined service level agreements for particular customers to affect the queuing function. A customer can be provided a higher quality of telecommunications service by, for example, paying additional money to receive such premium service. An algorithm running on module **1562** can increase the queuing priority for messages transmitted to such customers.

Virtual private network (VPN) directory enabled networking (DEN) data table **1572** can provide prioritization for a predetermined quality of service for a VPN for a company that pays for the VPN function. A VPN is understood by those skilled in the relevant art to be a private network, including a guaranteed allocation of bandwidth on the network, provided by the telecommunications service provider. VPN DEN data table **1572** permits module **1562** to provide higher quality of service for customer-purchased VPNs. As with SLA priority data table **1570**, the queuing priority can be increased for such VPNs. For example, a platinum level VPN's lowest priority IP flow classes could also be given a higher priority than a high priority brass level VPN.

Both SLA priority data table **1570** and VPN DEN data table **1572** receive input from operations, administration, maintenance and provisioning (OAM&P) module **1108**. This is a module that is kept off-line, and includes storage and revision of administrative information regarding new customers, or updates of information pertaining to existing customers. For example, the SLA priority of the customers and VPN information is updated from OAM&P module **1108**.

Hierarchical class-based priority processor module **1574** is a module that operates under the principles of hierarchical class-based queuing. Hierarchical class-based queuing was created by Sally Floyd and Van Jacobson, considered early architects of the Internet.

Hierarchical class-based queuing classifies different types of IP flows using a tree structure at the edge access device routers. Each branch of the tree signifies a different class of IP flows, and each class is dedicated a set limited amount of bandwidth. In this manner, different classes of flows are guaranteed minimum bandwidth, so that no single IP data flow within a class, and no single class of IP flows, can use up all available bandwidth. The present invention adds a prioritization feature enabling class based priority reservations to be made using the hierarchical class queue concept, as discussed above with respect to FIGS. **13** and **14**.

MAC downlink subframe scheduler **1566** is a processor module that takes the packets queued in class queues **1564***a*–**1564***f*, and can make frame slot reservations to fill up subframes **1568***a*–**1568***k* based on priorities **1570**, **1572** and **1574**, which is a variable number of frames. In one embodiment, each subframe is scheduled (filled) with up to a predetermined number of packets from each of the classes **1564***a*–**1564***f* according to priorities **1570**, **1572** and **1574**. In another embodiment, the subframes are scheduled according to the inventive advanced reservation algorithm method described with respect to FIGS. **13** and **14** for isochronous reservations. In yet another embodiment, the subframes are scheduled according to a combination of known methods and the advanced reservation algorithm method of the present invention.

The subframes can then be sent to WAP antenna **290***d* for wireless transmission over the wireless medium to RF transceiver subscriber antenna **292***d* coupled to subscriber CPE station **294***d*, which in turn can send the packets contained in the subframes to subscriber workstation **120***d* at CPE subscriber location **306***d*. The subframes can be scheduled from highest priority to lowest priority.

Hierarchical class-based priority (HCBP) processor module **1574** receives as input the subframes that have been scheduled and transmitted from WAP antenna **290***d*. By maintaining awareness of the status of the packets (i.e., by knowing which packets have been sent out), HCBP processor module **1574** knows which packets from which class queues **1564***a*–**1564***f* must yet be scheduled.

Every once in a while, a packet is lost through, e.g., noise. When this situation arises, the subscriber CPE station **294***d* sends a retransmit request **1576** to WAP **290***d*, which transmits the request to link layer acknowledgment (ARQ) processor **1578**. ARQ processor **1578** informs MAC downlink subframe scheduler **1566** of this condition, which in turn reschedules the requested packets from the appropriate class queues **1564***a*–**1564***f* for retransmission. Link layer acknowledgment ARQ processor **1578** also awaits positive acknowledgments from subscriber CPE station **294***d*, to determine that the data packets have been properly received. Only after receiving a positive receipt acknowledgment does MAC downlink subframe scheduler **1566** remove the packet from class queues **1564***a*–**1564***f*.

Each subscriber CPE station **294***d* has a limited amount of memory available for received data packets in an IP flow. When, for example, the devices coupled to the subscriber CPE station **294***d* (e.g., subscriber workstation **120***d*) stop receiving IP data flows (e.g., subscriber workstation **120***d* goes down), the CPE data packet queues in CPE subscriber station **294***d* are quickly filled up. In this scenario, subscriber CPE station **294***d* transmits a CPE IP flow queue depth message **1580** indicating that the queue is filled up, which can be received by CPE IP flow queue depth status processor **1582**. CPE queue depth processor **1582** informs MAC downlink subframe scheduler **1566** of this condition, which stops scheduling downlink subframes directed to subscriber CPE station **294***d*. Processor **1582** can also send messages to MAC downlink subframe scheduler **1566** to flush particular IP flows from class queues **1564***a*–**1564***f*.

h. Uplink SubFrame Prioritization

1. Overview

FIGS. **16**A and **16**B are exemplary logical flow diagrams for the uplink. The logical flow pertains to analysis and scheduling of shared wireless bandwidth to IP packet flows from a subscriber workstation **120***d* coupled to a subscriber CPE station **294***d*, being transmitted over the wireless medium up to the wireless base station **302**, and on to data network **142** for transmission to a destination host workstation **136***a*. FIG. **16**A is an exemplary logical flow diagram **1600** for uplink IP flow analyzer **632**. FIG. **16**B is an exemplary logical flow diagram **1660** for the uplink flow scheduler **634**.

The functional components for FIGS. **16**A and **16**B are explained by way of method modules, which can be viewed

as physical units (e.g., comprising software, hardware, or a combination thereof) or logical vehicles (e.g., used for explanatory purposes only). Those skilled in the art will recognize that the modules are used only to explain an exemplary embodiment, and are not to be considered limiting.

The exemplary logical flow diagram **1600** for uplink IP flow analyzer **632** of FIG. **16**A includes packet header identification component **1602**, packet characterization component **1604**, packet classification component **1606**, and IP flow presentation component **1608**. The functions of these components are explained in detail below.

In one embodiment, uplink IP flow analyzer **632** is physically located in wireless base station **302**, although those skilled in the art will recognize that the same functionality can be located remotely from wireless base station **302**. In a preferred embodiment of the present invention, the function of IP flow analyzer **632** is performed at a subscriber CPE station **294***d* desiring an uplink reservation slot for uplinking a packet/IP flow up to base station **302**. A reservation request block (RRB) request detailing the IP flow identifier, number of packets and classification of the IP flow can be created then by IP flow analyzer **632** and can be uplinked via preferably a contention RRB slot for scheduling by uplink frame scheduler **634** in future uplink subframe slots up at wireless base station **302**.

FIGS. **2**D, **3**A and **3**B are helpful to the reader for an understanding of the uplink IP flow analyzer.

2. Introduction

IP flow analyzer **632** performs the function of identifying, characterizing, classifying, and presenting data packets to an uplink frame scheduler **634**. The functions of identifying, characterizing, classifying and presenting the data packets can be respectively performed by packet header identification component **1602**, packet characterization component **1604**, packet classification component **1606** and IP flow presentation component **1608** of uplink IP flow analyzer **632**.

Packet header identification component **1602** determines whether a packet of an incoming IP flow is known to the system (i.e. is an existing IP flow), or if it is the first data packet of a new IP data flow, and determines the source application based on fields in the header section of the packet. Identification **1602** can include buffering packets and extracting and parsing the header contents. Packet characterization component **1604** characterizes a new data packet (of a new IP flow) to determine the QoS requirements for the IP flow based on the source application, and to identify the subscriber CPE station that will receive the IP flow. Packet classification component **1606** classifies the new IP data flow into one of several priority classes. Classification **1606** can include, e.g., grouping packets having similar QoS requirements. IP data flow presentation **1608** initializes the new IP data flow and presents it to uplink flow scheduler **634**.

Each time a subscriber CPE station **294***d* attempts to communicate in the uplink direction with wireless base station **302**, it requests a reservation by inserting an RRB in the uplink subframe. Uplink frame scheduler **634** then schedules the reservation request in a future uplink subframe and notifies the CPE station **294***d* of the reservation. In a downlink signal, uplink flow scheduler **634** located preferably at wireless base station **302**, transmits a reservation slot in a particular future frame for the requesting subscriber CPE station **294***d* to transmit its uplink data. Uplink flow scheduler **634** assigns the reservation based on the same parameters as the downlink flow scheduler **604** uses in the downlink. In other words, uplink flow scheduler **634** determines the reservation slots based on the queue class priority and based on a set of rules, schedules the reservations for uplink transmissions from subscriber CPE station **294***d* using, e.g., an advanced reservation algorithm. The rules are determined by inputs to the uplink flow scheduler **634** from a hierarchical class-based priority processor module **1674**, a virtual private network (VPN) directory enabled (DEN) data table **1672**, and a service level agreement (SLA) priority data table **1670**. The advanced reservation algorithm is described with respect to FIG. **14**.

3. Identification

Packet header identification component **1602** identifies the IP flow received from a subscriber CPE station **294***d* based on the packet's header contents.

A stream of packets, also known as packets from several IP flows (i.e. each IP flow is associated with a single "call") is received at packet header identification component **1602**. The IP flow in one embodiment is transmitted to subscriber CPE station **294***d* from one or more subscriber workstations **120***d* for uplink to host computers **136***a* coupled to wireless base station **302** by data network **142**. Subscriber CPE station **294***d* can transmit the data packets of the IP flow to packet buffer module **1610** of packet header identification component **1602**. In one embodiment, packet header identification component is within CPE subscriber station **294***d*. At module **1610**, the received packets are buffered in a storage area for transfer to header extraction module **1620**. At module **1620**, the packet header files are extracted and parsed to obtain the contents of the packet header fields.

Relevant fields can include, e.g., source, destination, type of service (TOS) and differentiated service (DiffServ) markings, if any exist.

For IP flows known to the system, there are entries in existing IP flow identification table **1626**. An IP flow is in the system if a previous packet of the IP flow of the existing IP data call has already been identified. In module **1622**, it is determined if there is a match between the incoming IP flow and an entry in table **1626**. If so, then the IP flow is known to the system, and control passes to module **1630** of the packet characterization component **1604**.

If the IP flow is not an existing flow known to the system, meaning that the IP flow is a new IP flow, then control passes to module **1624**, where the packet header fields are analyzed to identify the source application of the IP flow.

Packet header analysis module **1624** determines from source application packet header table **1628** the type of source application making the IP flow. The application can be any of the types of applications described with respect to FIG. **2**D or known to those skilled in the art. Examples include a file transfer protocol (FTP) download from another client workstation **138***f*, a voice telephony call from a caller **124***d* (connected over a modem), a fax machine call, and a conference call from multiple callers **124***d* and **126***d* (connected over a modem), to name a few. If the IP flow is a new IP flow, then the identification information about the new IP flow is added to table **1626**, and control passes from analysis module **1624** to module **1632** of the packet characterization component **1604**.

4. Characterization

Packet characterization component **1604** characterizes the IP flow and passes it to packet classification component **1606** for classification.

If the IP flow is an existing IP flow, control passes to module **1630** from module **1622** of the packet header identification component **1602**. If in module **1622** it is determined that the IP data flow is known to the system, in

module **1630** it is determined whether the packet is old (i.e., stale). This can include determining from a time-to-live field (a field in the IP packet header) the age of the packet, and comparing the field to a threshold age value. If the packet is determined to be stale, it is discarded. Module **1630** can anticipate application packet discards. From module **1630**, control passes to module **1640** of the packet classification component **1606**.

If the IP flow is new, control passes to module **1632** from module **1624** of the packet header identification component **1602**. If in module **1624** it is determined that the application associated with the IP flow application is not known to the system, in IP flow QoS requirements lookup module **1632** the QoS requirements for the application associated with the IP flow are determined. Module **1632** performs this operation by looking up the application in IP flow QoS requirement table **1634**. Different applications have different requirements. For example, bandwidth allocation (i.e., allocating an appropriate amount of bandwidth) is important to an application performing FTP downloads, and not jitter (i.e., time synchronizing the received data) and latency (i.e., the amount of time passage between responses). On the other hand, jitter and latency are important to voice telephony and conference calls, and bandwidth allocation is not.

After processing by module **1632**, control passes to module **163***b*. In CPE subscriber station identifier (ID) lookup module **1636** a subscriber CPE ID lookup is performed for the new IP data flow. Each subscriber CPE station **294***d* can have one or more applications, running on one or more subscriber workstations **120***d*, homed to it. Accordingly, one or many subscribers can generate or receive an IP flow directed from or at a subscriber CPE station **294***d*. A subscriber workstation **120***d* can be any device coupled to a subscriber CPE station **294***d*. Module **1636** looks up the CPE station identifier for the IP flow in table **1638**, to provide the CPE ID in the reservation request block (RRB). Control then passes from module **1636** to module **1648** of the packet classification component **1606**.

5. Classification

Packet classification component **1606** classifies the IP flow and passes it to IP flow presentation component **1608** for presentment.

For existing IP flows, control passes to module **1640** from module **1630** of the packet characterization component **1604**. If in module **1630** it is determined that the packet is not stale, then in module **1640** the packet is associated with its IP flow. As illustrated in FIG. **16**A, the packet processed herein was determined to be a portion of an IP flow known to the system. Therefore, the QoS processing of modules **1632**, **1636** and **1642** are unnecessary, because the QoS requirements of the present packet are the same as for its IP flow.

For new IP flows, control passes to module **1642** from module **1636** of the packet characterization component **1604**. In module **1642** the packet is classified or grouped into a QoS class by performing an IP flow QoS requirement table **1644** lookup where the QoS classes are stored depending on the QoS requirements for packets. From module **1642**, control passes to module **1648** of IP flow presentation component **1608**.

6. IP Flow Presentation

IP flow presentation component **1608** prepares and presents the IP data flow packets to flow scheduler **634**. In one embodiment of the uplink direction, a reservation request block (RRB) is created and uplinked via a contention slot to the wireless base station **302** for scheduling by IP flow scheduler **634**. In another embodiment, the scheduler is located at the CPE station **294***d* so no reservation request is needed.

For existing IP flows, control passes to module **1646** from module **1640** of the packet classification component **1640**. In module **1646**, the packet is added to the IP flow queue, which is the queue for the current existing IP flow. In one embodiment, this can include preparation of a RRB. From module **1646**, control passes to module **1662** of uplink flow scheduler **634**. In one embodiment, this can include uplink of the RRB from CPE **294***d* to wireless base station **302**.

For a new IP flow, control passes to module **1648** from module **1642** of the packet classification component **1606**. In initialize IP flow module **1648**, this new IP flow is initialized for presentation to module **1652**. Module **1652** presents the IP data flow (in particular, the reservation request block data packet) to module **1662** of uplink flow scheduler **634**. In module **1650**, the QoS class for the IP flow is presented to scheduler **634**, preferably by inclusion in a RRB.

7. Uplink Flow Scheduler

The exemplary logical flow diagram for the uplink flow scheduler **634** of FIG. **16**B comprises IP flow QoS class queuing processor module **1662**, MAC uplink subframe scheduler module **1666**, hierarchical class-based priority processor module **1674**, VPN DEN data table module **1672**, SLA priority data table **1670**, CPE IP flow queue depth status processor **1682** and link layer acknowledgment processor module **1678**.

Uplink flow scheduler **634** of FIG. **16**B also includes QoS class queues for class 1, **1664***a*; class 2, **1664***b*; class 3, **1664***c*; class 4, **1664***d*; class 5, **1664***e*; and class 6, **1664***f*; and

MAC uplink subframes: frame n **1668***a*; frame n+1, **1668***b*; frame n+2, **1668***c*; frame n+3, **1668***d*, . . . frame n+p, **1668***k*.

In one embodiment, uplink flow scheduler **634** is physically located in wireless base station **302**, although those skilled in the art will recognize that the same functionality can be located remotely from wireless base station **302**. For example, in another embodiment, uplink flow scheduler **634** can be located at CPE station **294***d* and is in communication with other CPE stations **294** and the wireless base station **302**.

Uplink flow scheduler **634** is used to schedule the uplink subframe. The entire frame is divided into an uplink portion (called an uplink subframe) for transmitting uplink frames, and a downlink portion (called a downlink subframe) for transmitting downlink frames.

Illustrated in FIG. **16**B are WAP antenna **290***d*, the wireless medium, RF transceiver subscriber antenna **292***d*, subscriber CPE station **294***d* and subscriber workstation **120***d*. WAP **290***d* and RF transceiver subscriber antenna **292***d* respectively provide a wireless connection between wireless base station **302** (where uplink flow scheduler **634** resides in one embodiment) and subscriber CPE station **294***d*, which can transmit upstream an IP flow from an application running on client computer **120***d*. WAP **290***d* serves as a wireless gateway for data network **142**, and RF transceiver subscriber antenna **292***d* serves as a wireless gateway for subscriber CPE station **294***d* to uplink the IP flow packet data.

Also illustrated in FIG. **16**B is data interface **320**, which provides a connection from uplink flow scheduler **634** for sending uplinked IP flow packets on to data router **140***d* of data network **142** and on to a destination host computer **136***a*. These connections are also illustrated in FIGS. **2**D and **3**B.

The previous frame includes an uplink reservation request which is received by the wireless base station from a

subscriber CPE station **294***d*. At this point, the reservation request block has been identified, characterized, classified, and presented, preferably at the CPE station **294***d*, and has been transmitted to uplink flow scheduler **634** from uplink flow analyzer **632** at the CPE **294***d*. In particular, the reservation request block is presented to IP flow QoS class queuing processor module **1662** from module **1650**. Module **1662** informs MAC uplink subframe scheduler **1666** of the reservation.

In turn, MAC uplink subframe scheduler **1666** uses a slot in the subframe to acknowledge receipt of the request called the acknowledgment request block (ARB). An exemplary slot used to convey the frame, slot, and IP flow identifier for this reservation is described with respect to FIG. **12**. Scheduler **1666** transmits in this reservation slot the CPE identification data, along with which future slot(s) and frame(s) the requesting subscriber CPE station **294***d* is permitted to use for uplink of the requested data packet IP flow transmissions.

The future slot(s) in the future frame(s) are assigned, e.g., based on inputs from hierarchical class-based priority processor module **1674**, VPN DEN data table **1672** and service level agreement (SLA) priority data table **1670**. These components function in a similar manner to hierarchical class-based priority processor module **1574**, VPN DEN data table **1572** and service level agreement (SLA) priority data table **1570**, described with respect to the downlink flow scheduler **604**.

When IP flow QoS class queuing processor module **1662** receives packets of an existing or new IP flow from IP flow presentation module **1608**, it then creates class queues **1664***a*–**1664***f*, which is a variable number of queues, and places the packets in these class queues. In a preferred embodiment there are between 3 and 10 classes. These queues hold reservation request packets for scheduling. Packets are placed in class queues **1664***a*–**1664***f* according to the contents of the reservation request block for input to module **1662**.

Module **1662** receives inputs from hierarchical class-based priority processor module **1674**, VPN DEN data table **1672** and service level agreement (SLA) priority data table **1670**. The queuing function of module **1662** is based on these inputs. These components function analogously to their counterparts in the downlink flow scheduling method. SLA priority data table **1670** and VPN DEN data table **1672** receive input from operations, administration, maintenance and provisioning (OAM&P) module **1108**. OAM&P module **1108** provides updates to priorities when, e.g., a subscriber modifies its service level agreement or a VPN subscription is changed.

MAC uplink subframe scheduler **1666** takes the requests queued in class queues **1664***a*–**1664***f*, and schedules reservations of slots in frames **1668***a*–**1668***k*, which is a variable number of frames. In one embodiment, each frame is scheduled with up to a predetermined number limit or percentage limit of packets from each of the classes **1664***a*–**1664***f*. The requests can be scheduled as shown in FIG. **13**, taking into account certain priorities. In another embodiment, the frames are scheduled according to the inventive advanced reservation algorithm method for scheduling isochronous type traffic described with respect to FIG. **14**. In yet another embodiment, the frames are scheduled according to a combination of known methods and the advanced reservation algorithm method of the present invention.

The reservation slot schedule can then be sent down to the CPE stations **294** using, e.g., FDB slots such as **1236***g* and **1236***h* of FIG. **12F**. The uplink slots can then be inserted by CPE station **294***d* into the uplink subframe as scheduled. The frame slots are then transmitted up from CPE station **294***d* to wireless base station **302** and are then sent on as packets to their destination addresses. For example, from wireless base station **302** the packets can be transmitted over data network **142** to a host computer **136***a*.

After the uplink packets are received by the wireless base station **302**, the wireless base station **302** sends an upstream acknowledgment data block (UAB) message back down to the transmitting subscriber CPE station **294***d*, to acknowledge receipt of the transmitted data packets.

Every once in a while, a packet is lost through noise or other interference in the wireless medium. When this situation arises, the subscriber CPE station **294***d* determines that it has not received a UAB data acknowledgment, so it sends a retransmit request requesting another uplink reservation slot to wireless base station **302** via WAP **290***d*, which transmits the request to link layer acknowledgment (ARQ) processor **1678**. ARQ processor **1678** informs MAC uplink subframe scheduler **1666** of the need of retransmission (i.e. the need of a frame slot reservation for resending the uplink packet). CPE subscriber station **294***d* can also send to ARQ processor **1678**, other data messages about nonreceipt of uplink transmission acknowledgments. The ARQ **1678** can forward such messages on to the uplink subframe scheduler **1666**. The uplink subframe scheduler **1666** in turn reschedules the requested uplink reservation from the appropriate class queues **1664***a*–**1664***f*. Alternatively, in another embodiment, link layer acknowledgment processor **1678** can also send a positive UAB acknowledgment to the subscriber CPE station **294***d*, to indicate that the data packets have been properly received. Thus uplink scheduler **1666** in addition to scheduling first time reservations, also can schedule repeat reservations for lost packets.

Each subscriber CPE station **294***d* has a limited amount of memory space available for queuing packets received from subscriber workstations **120***d* awaiting reservation slots of uplink from the CPE **294***d* to wireless base station **302**. When, for example, the the queue of subscriber CPE station **294***d* becomes full from a backup of packets awaiting upstream reservations, IP data flows can potentially be lost, or packets may become stale. In this scenario, subscriber CPE station **294***d* transmits a CPE IP flow queue depth message **1680** to the wireless base station **302** indicating that the queue is filled up, which can be received by CPE IP flow queue depth status processor **1682**. Processor **1682** can inform MAC uplink subframe scheduler **1666** of this condition, which can, e.g., increase temporarily the priority of IP flows at subscriber CPE station **294***d* to overcome the backlog or can, e.g., stop transmitting additional downlink packets to the CPE station **294***d* until the queue depth backlog is decreased to an acceptable level again. Processor **1682** can also send messages to MAC uplink subframe scheduler **1666** to flush reservation requests from the subscriber CPE station **294***d* in class queues **1664***a*–**1664***f*.

4. TCP Adjunct Agent

TCP is a reliable transport protocol tuned to perform well in traditional networks where congestion is the primary cause of packet loss. However, networks with wireless links incur significant losses due to bit-errors. The wireless environment violates many assumptions made by TCP, causing degraded end-to-end performance. See for example, Balakrishnan, H., Seshan, S. and Katz, R. H., "Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks," University of California at Berkeley, Berkeley, Calif., accessible over the Internet at URL, http://

www.cs.berkeley.edu/~ss/papers/winet/html/winet.html, dealing more directly with handoffs and bit errors in a narrowband wireless environment, the contents of which are incorporated by reference. Attempts to address this problem have modified TCP in order to overcome it. However, this is not a commercially feasible means of overcoming this challenge. It is impracticable to implement any solution that requires a change to the standard operation of TCP.

The present invention uses an enhanced MAC layer which interfaces with a TCP adjunct agent to intercept TCP layer requests to manipulate the TCP layers at either a source or destination end of a transmission, to modify TCP behavior at the source and destination of the TCP/IP transmission which includes an intermediary wireless link. Packets can be queued at the wireless base station awaiting receipt acknowledgment and the base station can perform local retransmissions across the wireless link to overcome packet loss caused by high bit-error rates. Communication over wireless links is characterized by limited bandwidth, high latencies, sporadic high bit-error rates and temporary disconnections which must be dealt with by network protocols and applications.

Reliable transport protocols such as TCP have been tuned for traditional wired line networks. TCP performs very well on such networks by adapting to end-to-end delays and packet losses caused by congestion. TCP provides reliability by maintaining a running average of estimated round-trip delay and mean deviation, and by retransmitting any packet whose acknowledgment is not received within four times the deviation from the average. Due to the relatively low bit-error rates over wired networks, all packet losses are correctly assumed to be caused by congestion.

In the presence of the high bit-error rates characteristic of wireless environments, TCP reacts to packet losses as it would in the wired environment, i.e. it drops its transmission window size before retransmitting packets, initiates congestion control or avoidance mechanisms (e.g., slow start) and resets its retransmission timer. These measures result in an unnecessary reduction in the link's bandwidth utilization, thereby causing a significant degradation in performance in the form of poor throughput and very high interactive delays.

The present invention maintains packets in class queues awaiting acknowledgment of receipt from the subscriber CPE stations. Unacknowledged data slots can then be resent by having the wireless base station perform local retransmissions to the subscriber CPE station. By using duplicate acknowledgments to identify a packet loss and performing local retransmissions as soon as the loss is detected, the wireless base station can shield the sender from the inherently high bit error rate of the wireless link. In particular, transient situations of very low communication quality and temporary disconnectivity can be hidden from the sender.

For transfer of data from a CPE subscriber host to a wireless base station host, missing packets are detected at the wireless base station and negative acknowledgments can be generated for them. The negative acknowledgments can request that the packet be resent from the CPE subscriber host (the sender). The CPE subscriber host can then process the negative acknowledgment and retransmit corresponding missing packets. Advantageously, no modifications to the sender TCP or receiver TCP is necessary, since the present invention places TCP aware functionality in the MAC layer.

FIG. **5A** illustrates flow **500** depicting IP flows from a source TCP at a subscriber host, down a protocol stack for transmission through a CPE subscriber station, through a wireless medium to a wireless base station, up and through a protocol stack at the wireless base station having an example TCP adjunct agent, then through a wireline connection and through a protocol stack to a destination host. The adjunct TCP agent modifies operation of a TCP sliding window algorithm at the transmitting TCP and in cooperation with proactive reservation-based intelligent multimedia access technology (PRIMMA) media access control (MAC) enables local retransmission over the wireless medium in accord with the present invention.

Specifically, flow **500** illustrates IP packet flow from subscriber workstation **120***d*, through CPE subscriber station **294***d* at CPE subscriber location **306***d*, then over a wireless transmission medium to wireless base station **302**, and eventually over a wireline link over data network **142** to host workstation **136***a*.

TCP adjunct agent **510***e* makes sure transport is reliable by modifying operation of the TCP sliding window algorithm at the transmitting TCP in a manner that optimizes the window for the wireless medium. TCP adjunct agent **510***e* advantageously is transparent to industry standard protocols as agent **510***e* does not require modification of the standard TCP/UDP layer of client subscriber workstation **120***d* or host workstation **136***a*.

Flow **500** includes IP flows from application layer **512***a*, down the protocol stack through TCP/UDP layer **510***a*, through IP layer **508***a*, then through point-to-point (PPP) layer **520***a*, then through data link Ethernet layer **504***a*, then through 10BaseT Ethernet network interface card (NIC) physical layer **502***a*, over a wire line connection to 10BaseT Ethernet NIC physical layer **502***b* of subscriber CPE **294***d*.

Subscriber CPE **294***d* flows packets coming in from NIC **502***b*, back up its protocol stack through Ethernet layer **504***b*, through PPP layers **520***b* and **520***c*, back down through PRIMMA MAC **504***c* to wireless physical layer **502***c* including antenna **292***d*, then over the wireless medium to antenna **290***d* of wireless base station **302**.

Wireless base station **302** flows packet IP flows up from antenna **290***d* at physical layer **502***d* through PRIMMA MAC layer **504***d*, through PPP layer **520***a*, through IP layer **508***d* to TCP adjunct agent **510***e*, which can flow IP flows down through IP layer **508***e*, through PPP layer **520***e*, through wide area network (WAN) layer **504***e*, through wireline physical layer **502***e*, through interface **320**, over routers **140***d*, through data network **142**, via wireline connections to wireline layer **502***f* of WAN host workstation **136***a*.

Host workstation **136***a* flows IP flows from wireline layer **502***f*, up through its protocol stack through WAN layer **504***f*, through PPP layer **520***f*, through IP layer **508***f*, to TCP/UDP layer **510***f* and on to application layer **512***f*.

TCP/UDP layers **510***a* and **510***f* act to provide such transport functions as, e.g., segmentation, managing a transmission window, resequencing, and requesting retransmission of lost packet flows. Normally TCP layers **510***a* and **510***f* would send a window of packets and then await acknowledgment or requests for retransmission. A TCP sliding window algorithm is normally used to vary the transmission flow to provide optimized transport and to back off when congestion is detected by receipt of requests for retransmission. Unfortunately in the wireless environment, due to high bit error rates, not all packets may reach the destination address, not because of congestion, but rather because of high bit error rates, so as to prompt a retransmission request from the destination IP host to the source. Rather than slow transport, TCP adjunct agent **510***e* modifies operation of the TCP sliding window algorithm to optimize operation over wireless. PRIMMA MAC layer **504***d* inter-

acts with TCP adjunct agent **510***e* permitting the agent to intercept, e.g., retransmission requests, from TCP layer **510***a* of subscriber workstation **120***d* intended for host **136***a*, and allowing the wireless base station to retransmit the desired packets or flows to subscriber workstation **120***d* rather than forwarding on the retransmission request to host **136***a*, since the packets could still be stored in the queue of PRIMMA **504***d* and would not be discarded until an acknowledgment of receipt is received from the subscriber CPE. Since retransmission can be performed according to the present invention at the PRIMMA MAC data link layer, i.e. layer 2, retransmission can occur from the base station to the CPE subscriber, rather than requiring a retransmission from all the way over at the transmitting source TCP which would cause TCP to backoff its sliding window algorithm. Thus, by having wireless base station **302** retransmit until receipt is acknowledged over the wireless link, the inherently high bit error rate can be overcome, while maintaining an optimal TCP window.

Recall, a TCP transmitter transmits a TCP sliding window block of packets and alters the size of the window upon detection of congestion. The TCP transmitter transports a block of packets in a window, and then awaits acknowledgment from the receiver. If transmission is going smoothly, i.e. no congestion or lost packets occur, then the transmitter TCP ramps up the transmission rate. This increased transmission rate continues until the transmitting TCP detects congestion or packet loss. When notified of congestion, the transmitting TCP stops transmitting, backs off and sends a smaller block (i.e. a smaller window) of packets.

TCP adjunct agent modifies normal TCP operation by tricking the transmitting TCP and its transmitting window algorithm. The TCP adjunct agent prevents the transmitter from being notified of loss, i.e. receiving congestion notification, from the receiving TCP by, e.g., preventing duplicate retransmission requests. Since the transmitting TCP does not receive such notification, it does not modify the TCP sliding window and transmission continues at the higher rate.

In the event that real congestion occurs, i.e. if the TCP adjunct agent recognizes packets really were lost, then the TCP adjunct agent can let the retransmission request go through to the transmitting TCP. This is advantageously accomplished because the MAC link layer of the present invention is in communication with the higher protocol layers, it is application aware, transport aware and network aware. In this case, because the MAC layer is transport layer aware, PRIMMA MAC layer **504***d* communicates with the TCP adjunct agent **510***e* at layer 4. Since the MAC requires acknowledgment of receipt of wireless transmissions sent to the CPE subscriber station **294***d* for every packet sent from the wireless base station **302**, the MAC layer **504***d* knows whether an inter-TCP layer communication, e.g., a request for retransmission, is sent from a client computer TCP at the CPE station is created because the lost packet was lost in wireless transmission, or because of real congestion.

If PRIMMA MAC **504***d* does not receive an acknowledgment from **504***c*, then the PRIMMA MAC **504***d* of wireless base station **302** can retransmit the contents of the lost packet to the subscriber CPE station **294***d*. If the PRIMMA MAC **504***c* of the subscriber CPE station **294***d* acknowledges receipt and still requests a retransmission, then real congestion could have occurred and the PRIMMA MAC **504***d* of the wireless base station **302** can let the TCP adjunct agent **510***e* know that it should allow the retransmission request to be sent to the transmitting TCP **510***f* of host workstation **136***a*.

Thus, TCP adjunct agent **510***e* of the present invention can modify operation of the TCP sliding window algorithm in a manner that is optimal for the wireless medium, without requiring any change to commercially available TCP layers **510***a* and **510***f* at the receiver and sender hosts. In an embodiment, TCP adjunct agent **510***e* obviates the need for any modification of the TCP layers at either the sending (i.e. transmitting) host or client. In another embodiment the host and client TCP layers are unaware of the modification of operation by the TCP adjunct agent, i.e. it is transparent to source and destination TCP layers. In another embodiment, TCP adjunct agent **510***e* intercepts retransmission requests between a TCP layer of the client computer coupled to the subscriber CPE station and the TCP layer of the host workstation coupled to the data network.

FIG. **5**B illustrates functional flow diagram **522** including an example functional description of TCP adjunct agent **510***e* performing an outgoing TCP spoof function. Referring to FIGS. **5**B and **5**A, diagram **522** assumes that a TCP layer **510***f* at a transmitting host **136***a* has transmitted a windowful of packet data to subscriber workstation **120***d*, and awaits acknowledgment. Diagram **522** illustrates receipt of an outgoing TCP message **524** in TCP adjunct agent **510***e* at wireless base station **302** which has been sent from subscriber workstation **120***d* via subscriber CPE station **294***d*.

In step **526**, the TCP header contents of outgoing TCP message **524** is parsed in order to reveal the contents of the message being sent from subscriber workstation **120***d* through the wireless network toward the transmitting host **136***a*.

In step **528**, it is determined whether the TCP header contents includes a duplicate acknowledgment message from the CPE station. Receiving a duplicate acknowledgment request from the CPE subscriber location could be indicative of a lost message in the wireless medium, or a real congestion problem. If in step **528** the TCP packet is determined to be a duplicate acknowledgment message, then processing can continue with step **532**, if not, then processing can continue with step **530**.

In step **530**, it is determined that there was real congestion, i.e., this was not a duplicate acknowledgment message caused by retransmission attempts at the wireless link layer. Thus, in step **530**, the TCP message is permitted to pass through TCP adjunct **510***e* without modification, and can continue through flow **500** to TCP layer **510***f* of FIG. **5**A.

In step **532**, since there was a duplicate acknowledgment detected in step **528**, it is determined whether the packet was successfully transmitted, or not. Step **532** is performed via intercommunication between TCP adjunct agent **510***e* and PRIMMA MAC layer **504***d*. This is an example of the interactivity between PRIMMA MAC and higher layer protocols illustrated as line **428** in FIG. **4**. PRIMMA MAC layer **504***d* can identify whether a packet was successfully sent from wireless base station **302** to CPE station **294***d* since, as illustrated in FIG. **15**B, requests for retransmission **1576** are received from CPE station **294***d* at link layer acknowledgment (ARQ) processor **1578** to MAC downlink subframe scheduler **1566** alerting the scheduler **1566** to retransmit the lost packet in a future frame **1568**. If in step **532**, it is determined that the packet was successfully transmitted, then processing can continue with step **530**, as described above. If however it is determined that the packet was not successfully transmitted, then processing continues with step **534**.

In step **534**, since the packet was not successfully transmitted, TCP adjunct agent **510***e* can suppress transmission of TCP message **524** since it can be assumed that the

packet was lost in the wireless medium. Processing can continue with step **536**.

In step **536**, TCP adjunct agent **510***e* can wait for notification from PRIMMA MAC **504***d* that a successful link layer retransmission of the lost packet was received at link layer acknowledgment processor **1578**. From step **536**, processing can continue with step **538**.

In step **538**, upon receipt of acknowledgment of a successful PRIMMA MAC **504***d* link layer retransmission, then normal TCP messages can be resumed.

In another step (not shown), TCP adjunct agent and PRIMMA MAC layers can set a limit of a threshold number of retransmission attempts, and if that threshold is reached, then processing can continue with step **530** to permit the TCP message to pass without modification.

FIG. **5**C illustrates functional flow diagram **540** including an example functional description of TCP adjunct agent **510***e* performing an incoming TCP spoof function. Referring to FIGS. **5**C and **5**A, diagram **540** assumes that a TCP layer **510***a* at a transmitting subscriber workstation **120***d* has transmitted a windowful of packet data to host **136***a*, and awaits acknowledgment. Diagram **544** illustrates receipt of an incoming TCP message **542** in TCP adjunct agent **510***e* at wireless base station **302** which has been sent from host workstation **136***a* via data network **142** for transmission over the wireless medium to subscriber CPE **294***d* to subscriber workstation **120***d*.

In step **544**, the TCP header contents of ingoing TCP message **542** is parsed in order to reveal the contents of the message being sent from host **136***a* through the wireless network toward the transmitting subscriber workstation **120***d*.

In step **546**, it is determined whether the TCP header contents includes a duplicate acknowledgment message from host **136***a*. Receiving a duplicate acknowledgment request from the host could be indicative of a lost message in the wireless medium, or a real congestion problem. If in step **546** the TCP packet is determined to be a duplicate acknowledgment message, then processing can continue with step **550**, if not, then processing can continue with step **548**.

In step **548**, it is determined that there was real congestion, i.e., this was not a duplicate acknowledgment message caused by retransmission attempts at the wireless link layer. Thus, in step **548**, the TCP message is permitted to pass through TCP adjunct **510***e* without modification, and can continue through flow **500** to TCP layer **510***a* of FIG. **5**A.

In step **550**, since there was a duplicate acknowledgment detected in step **546**, it can be determined whether the packet was successfully transmitted, or not. Step **550** can be performed via intercommunication between TCP adjunct agent **510***e* and PRIMMA MAC layer **504***d*. This is an example of the interactivity between PRIMMA MAC and higher layer protocols illustrated as line **428** in FIG. **4**. PRIMMA MAC layer **504***d* can identify whether a packet was successfully sent from CPE station **294***d* to wireless base station **302**, as illustrated in FIG. **16**B, requests for retransmission **1676** are received from CPE station **294***d* at link layer acknowledgment (ARQ) processor **1678** to MAC downlink subframe scheduler **1666** alerting the scheduler **1666** to retransmit the lost packet in a future frame **1668**. If in step **550**, it is determined that the packet was successfully transmitted, then processing can continue with step **548**, as described above. If however it is determined that the packet was not successfully transmitted, then processing continues with step **552**.

In step **552**, since the packet was not successfully transmitted, TCP adjunct agent **510***e* can suppress transmission of TCP message **542** since it can be assumed that the packet was lost in the wireless medium. Processing can continue with step **554**.

In step **554**, TCP adjunct agent **510***e* can wait for notification from PRIMMA MAC **504***d* that a successful link layer retransmission of the lost packet was received at link layer acknowledgment processor **1678**. From step **554**, processing can continue with step **556**.

In step **556**, upon receipt of acknowledgment of a successful PRIMMA MAC **504***d* link layer retransmission, then normal TCP messages can be resumed.

In another step (not shown), TCP adjunct agent and PRIMMA MAC layers can set a limit of a threshold number of retransmission attempts, and if that threshold is reached, then processing can continue with step **548** to permit the TCP message to pass without modification.

5. Wireless QoS Aware PRIMMA Media Access Control (MAC) Hardware Architecture

FIG. **10** illustratively depicts an embodiment of PRIMMA MAC hardware architecture **1000**. Architecture **1000** shows data network **142** coupled by a wireline bidirectional connection to WAN interface **320**.

WAN interface **320** is bidirectionally linked to a bidirectional data frame FIFO **1002** which is bidirectionally coupled to both segmentation and resequencing (SAR) **1004** and QoS/SLA rules engine and processor **1008**.

QoS/SLA rules engine and processor **1008** is also bidirectionally coupled to IP flow buffers **1014** and flash random access memory (RAM) **1010**.

SAR **1004** is bidirectionally coupled to IP flow buffers **1014**, flash RAM **1010**, QoS/SLA rules engine and processor **1008** and PRIMA MAC scheduler ASIC **1012**.

PRIMA MAC scheduler ASIC **1012** is also bidirectionally coupled to an RF interface **290**, a static RAM (SRAM) radio cell buffer **1018** and IP blow buffer **1014**.

6. Wireless Base Station Software Organization

FIG. **11** is an exemplary software organization for a packet-centric wireless point to multi-point telecommunications system. The software organization of FIG. **11** includes wireless transceiver and RF application specific integrated circuit (ASIC) module **290**, IP flow control component **1102**, WAN interface management component **1104**, QoS and SLA administration component **1106**, system and OAM&P component **1108**, customer billing and logging component **1110**, directory enabled networking (DEN) component **1112**, and wireless base station **320**.

IP flow control module **1102** includes transmission queuing control module **1102***a*, TCP rate control and class of service module **1102***b*, wireless PRIMMA MAC layer engine **1102***c* and IP flow identification and analysis module **1102***d*.

WAN interface management component **1104** includes WAN ingress/egress queuing control module **1104***a*, WAN interface ports (e.g., for T1, T3, OC3 ports) **1104***b*, firewall and security module **1104***c*, and WAN traffic shaping module **1104***d*.

The IP Flow control component **1102** and WAN interface management component **1104** represent the "core" of the system, where the packet processing, MAC layer scheduling, TCP proxy agent, and WAN I/F control functions are located. Much of the activities of the "non-core" components described above support and control these core components.

QoS and SLA administration component **1106** includes includes QoS performance monitoring and control module

1106*a*, service level agreements module 1106*b*, policy manager module 1106*c* and encryption administration module 1106*d*.

The QoS and SLA administration component 1106 provides the static data needed by the system in order to properly group particular IP-flows into QoS classes. Typically, during the provisioning phase of installing the system, the service provider will (remotely) download pertinent information about the subscriber CPE station 294, including the subscriber CPE stations's SLA, any policy-based information (such as hours of operation or peak data transmission rate allowance.). Encryption keys or "strengths" can also be downloaded, which may be subscriber CPE station or service provider specific.

System OAM&P component 1108 includes SNMP proxy client for WAP module 1108*a*, SNMP proxy clients for CPE module 1108*b*, and system operations, administration, management and provisioning module 1108*c*.

The OAM&P component 1108 allows remote service personnel and equipment to monitor, control, service, modify and repair the system. System performance levels can be automatically monitored, and system traps and traces can be set. Subscriber complaints can be addressed with the use of remote test and debug services controlled by OAM&P component 1108. System capacity limits can be monitored, and proactive provisioning of additional WAN connectivity can occur, as the result of automatic trend analysis functions in OAM&P component 1108.

Customer billing and logging module 1110 includes account logging and database management module 1110*a*, transaction query and processing control module 1110*b*, billing and account control module 111*c*, and user authentication module 1110*d*.

The customer billing and logging component 1110 allows the service provider to receive account, billing and transaction information pertaining to subscribers in the system. For service providers who bill on the basis of usage, cumulative system resource utilization data can be gathered. For specific types of activities (eg. video conferencing, multi-casting, etc.) there may be special billing data that is collected and transmitted to the service provider. This component also controls the availability of the system to subscribers through the operation of the subscriber authentication function. Once a subscriber is authorized to use the system, a new subscriber authentication entry is made (remotely) by the service provider. Likewise, a subscriber can be denied further access to the system for delinquent payment for services, or for other reasons. The service provider can also remotely query the system for specific account-related transactions.

Directory Enabled Networking (DEN) component 1112 includes DEN QoS 1112*a* module, DEN management and provisioning 1112*b* module, DEN IPSEC module 1112*c* and IP-based VPN control and administration module 1112*d*.

The DEN component 1112 allows the service provider the means to input into the system relevant information regarding the operation of DEN-based VPN's of subscribers. Subscriber VPNs need to be "initialized" and "provisioned" so that the system properly allocates system resources to subscribers with these VPNs, and provides for the recognition and operation of these VPNs. Data from DEN component 1112 are utilized by the system to apply the appropriate priorities to IP-flows of the subject subscribers.

The invention's packet-centric wireless base station supports directory enabled networking (DEN), a MICROSOFT, INTEL and CISCO standard for providing a standard structure for how distributed sites manage IP flows. The present invention prioritizes VPN traffic in a lightweight directory access protocol (LDAP)-compliant (LDAP is available from MICROSOFT of Redmond, Wash.) manner which allows remote administration, provisioning and management. The present invention is also LDAP version 2 compliant. The present invention also complies with the X.500 standard promulgated by the international telecommunications union/telecommunications section (ITU/T), and with the RFC 1777.

In one embodiment, DEN provides policy-based network management, IPsec compatible network security, and IPsec based VPNs. The DEN of the wireless base station 302 is planned to be common information model (CIM) 3.0 compatible (once the specification is finalized). The wireless base station 302 can provide native DEN support and supports directory based DEN QoS mechanisms including reservation model (i.e. RSVP, per-flow queuing), and precedence/priority/differentiated model (i.e. packet marking). Wireless base station 302 can plan support of DEN network policy QoS, and until DEN is complete, can support internal QoS and network extensions.

6. IPsec Support

IPsec is introduced above with reference to FIG. 4. IPsec provides a standard method of encrypting packets. In VPN tunnel mode, an entire header can be encoded, i.e. encrypted. In order for the present invention to be able to implement its packet-centric, QoS aware prioritization, during identification of a packet/IP flow, the wireless base station needs to be able to analyze the contents of header fields of the packets. Therefore, analysis of unencrypted packets is desirable.

The present invention already encrypts the data stream prior to transmitting frames over the wireless medium, so IPsec does not really need to be used over the wireless link to provide for encrypted transmission. Where a service provider finds it desirable to use IPsec, IPsec can be used for authentication and secure encapsulation of the header and payload, or just the payload data. IPsec is normally integrated at a firewall. If a service provider desires to implement the present invention and IPsec, then the present invention should be implemented behind the firewall, i.e. the firewall can be moved to the wireless base station. This permits ending the IPsec stream at the base station which can provide the base station access to packet header fields.

FIG. 17 illustrates IP flow in the downlink direction including IPsec encryption. Similarly, FIG. 18 illustratively depicts an uplink direction of IPsec support of the present invention.

FIG. 17 illustrates downlink flow 1700 depicting downlink direction IP flows from a source host workstation 136*a*, down a protocol stack which supports IPsec, for transmission up and through wireless base station 302 which is coupled to data network 142, through encryption layers, then through the wireless link to subscriber CPE 294*d*, up and through a protocol stack at the subscriber CPE 294*d*, then through a wireline connection to data network 142 and up through the protocol stack to the destination subscriber workstation 120*d* at subscriber location 306*d*.

Specifically, flow 1700 illustrates IP packet flow from host workstation 136*a*, through wireless base station 302, then over a wireless transmission link to subscriber CPE 294*d*, and over a wireline link to subscriber workstation 120*d*.

Host workstation 136*a* flows IP flows down from application layer 1712*h*, down through TCP/UDP layer 1710*h*, through IP layer 1708*h*, through optional PPP layer 1706*h*, through Ethernet layer 1705*h*, down through 10BaseT layer 1702*h*, over data network 142 to 10BaseT layer 1702*g*, then up through Ethernet 1704*g*, up its protocol stack through

optional PPP layer **1706***g* to IP layer **1708***g* and **1708***h*, back down through Internet firewall and IPsec security gateway **1706***f*, down through WAN layer **1704***f*, to wireline layer **1702***f* to data network **142** to wireline physical layer **1702***e*.

Wireline physical layer **1702***e* of wireless base station **302**, flows IP flows up the protocol stack through WAN layer **1704***e* through IPsec security gateway **1706***e* and firewall to IP network layer **1708***e* and **1708***d* and then down through encryption layer **1706***d*, PRIMMA MAC layer **1704***d* and down to wireless link to subscriber CPE **294***d*.

Subscriber CPE **294***d* flows packet IP flows up from antenna **292***d* at physical wireless layer **1702***c* up through MAC layer **1704***c*, through encryption layer **1706***c*, through IP layers **1708***b* and **1708***c*, then down through optional layer **1706***b* to Ethernet layer **1704***b* to 10BaseT connection **1702***b* to 10BaseT connection.

Subscriber workstation **120***d* flows IP flows up from 10BaseT layer **1702***a* up through its protocol stack through Ethernet layer **1704***a*, through optional PPP layer **1706***a*, through IP layer **1708***a*, to TCP/UDP layer **1710***a* and on up to application layer **1712***a*.

FIG. **18** illustrates uplink flow **1800** depicting uplink direction IP flows from a source TCP at subscriber workstation **120***d* at CPE location **306***d*, down a protocol stack for transmission through Ethernet coupled CPE subscriber station **294***d* through wireless medium to wireless base station **302**, up and through a protocol stack at the wireless base station **302** which supports IPsec, then through a wireline connection to data network **142** and through a protocol stack to a destination host.

Specifically, flow **1800** illustrates IP packet flow from subscriber workstation **120***d*, through subscriber CPE **294***d*, then over a wireless transmission medium to wireless base station **302**, and eventually over a wireline link to host workstation **136***a*.

Flow **1800** includes IP flows from application layer **1812***a*, down the protocol stack through TCP/UDP layer **1810***a*, through IP layer **1808***a*, then through optional point-to-point (PPP) layer **1806***a*, then through data link Ethernet layer **1804***a*, then through 10BaseT Ethernet network interface card (NIC) physical layer **1802***a*, over a wire line connection to 10BaseT Ethernet NIC physical layer **1802***b* of subscriber CPE **294***d*.

Subscriber CPE **294***d* flows packets coming in from NIC **1802***b*, back up its protocol stack through Ethernet layer **1804***b*, through optional PPP layer **1806***b* to IP layer **1808***b* and **1808***c*, back down through an Internet firewall and IPsec security gateway **1806***c*, down through PRIMMA MAC **1804***c* to wireless physical layer **1802***c* including antenna **292***d*, then over the wireless medium, such as, e.g., RF communication, cable RF, and satellite link, to antenna **290***d* of wireless base station **302** at wireless physical layer **1802***d*.

Wireless base station **302** flows packet IP flows up from antenna **290***d* at physical wireless layer **1802***d* up through MAC layer **1804***d*, through IPsec layers **1806***d* and **1806***d*, which can encapsulate packets and encrypt them. From IPsec layer **1806***e*, IP flows can flow down through WAN layer **1804***e* and through wireline physical layer **1802***e* over data network **142**.

Wireline physical layer **1802***f* flows IP flows up the protocol stack through WAN layer **1804***f* through IPsec security gateway **1806***f* and firewall to IP network layer **1808***f* and **1808***g* and then down through optional PPP layer **1806***h*, Ethernet layer **1804***h* and down through 10BaseT layer **1802***g*, through interface **320**, over routers **140***d*, through data network **142**, via wireline connections to 10BaseT physical layer **1802***h* of host workstation **136***a*.

Host workstation **136***a* flows IP flows up from 10BaseT layer **1802***h* up through its protocol stack through Ethernet layer **1805***h*, through optional PPP layer **1806***h*, through IP layer **1808***h*, to TCP/UDP layer **1810***h* and on to application layer **1812***h*.

IV. Conclusion

While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

What is claimed is:

1. An IP flow classification system that groups IP flows in a packet-centric wireless point to multi-point telecommunications system, said classification system comprising:

a wireless base station coupled to a first data network;

one or more host workstations coupled to said first data network;

one or more subscriber customer premise equipment (CPE) stations in wireless communication with said wireless base station over a shared bandwidth using a packet-centric protocol; and

one or more subscriber workstations coupled to each of said subscriber CPE stations over a second network;

resource allocation means optimizing end-user quality of service (QoS) and allocating shared bandwidth among said subscriber CPE stations; and

means for analyzing and scheduling an internet protocol (IP) flow over said shared wireless bandwidth, wherein said analyzing means comprises:

a classifier that classifies said IP flow.

2. The system of claim **1**, wherein said classifier comprises:

means for associating a packet of an existing IP flow with said IP flow.

3. The system of claim **1**, wherein said classifier comprises:

QoS grouping device that groups a packet of a new IP flow into a QoS class grouping.

4. The system of claim **3**, wherein said QoS grouping device comprises:

determining device that determines and takes into account QoS class groupings for said IP flow.

5. The system of claim **4**, wherein said QoS grouping device comprises:

optional differentiated services (Diff Serv) device that takes into account an optional Diff Servs field priority marking for said IP flow.

6. The system of claim **4**, wherein said QoS grouping device comprises:

optional type of service (TOS) device that takes into account any optional type of service field priority marking for said IP flow.

7. The system according to claim **1**, wherein said packet-centric protocol is transmission control protocol/internet protocol (TCP/IP).

8. The system according to claim **1**, wherein said packet-centric protocol is user datagram protocol/internet protocol (UDP/IP).

9. The system according to claim **1**, wherein said shared wireless bandwidth comprises a wireless communication medium comprising at least one of:

a radio frequency (RF) communications medium;

a cable communications medium; and

a satellite communications medium.

10. The system according to claim 9, wherein said wireless communication medium further comprises, a telecommunications access method including at least one of:

a time division multiple access (TDMA) access method;

a time division multiple access/time division duplex (TDMA/TDD) access method;

a code division multiple access (CDMA) access method; and

a frequency division multiple access (FDMA) access method.

11. The system according to claim 1, wherein said first data network comprises at least one of:

a wireline network;

a wireless network;

a local area network (LAN); and

a wide area network (WAN).

12. The system according to claim 1, wherein said second network comprises at least one of:

a wireline network;

a wireless network;

a local area network (LAN); and

a wide area network (WAN).

13. The system according to claim 1, wherein said resource allocation means optimizes end-user internet protocol (IP) quality of service (QoS).

14. The system according to claim 1, wherein said resource allocation means is application aware.

15. The system according to claim 1, wherein said IP flow includes at least one of:

a transmission control protocol/internet protocol (TCP/IP) flow, and

a user datagram protocol/internet protocol (UDP/IP) flow.

16. The system according to claim 1, wherein said analyzing and scheduling means further comprises at least one of:

an identifier operative to identify said IP flow,

a characterizer operative to characterize said IP flow, and

a prioritizer device operative to prioritize said IP flow.

17. The system according to claim 16, wherein said identifier comprises:

an analyzer device operative to analyze one or more header and payload packet fields; and

an identifier device operative to identify a new and an existing IP flow.

18. The system according to claim 17, wherein said analyzer device comprises:

a buffer operative to buffer packets of a plurality of IP flows;

a data extraction device operative to extract data from said one or more header and payload packet fields of each of said packets; and

a packet field analyzer device operative to analyze said header and payload packet fields.

19. The system according to claim 18, wherein said data extraction device comprises:

means for determining whether a packet of said IP flow is of version IPv.4 or IPv.6; and

means for parsing said packet of said IP flow.

20. The system according to claim 18, wherein said packet field analyzer comprises:

determining means for determining a source application type.

21. The system according to claim 18, wherein said data extraction device comprises:

an IP version determiner; and

a parser operative to parse said packets.

22. The system according to claim 18, wherein said packet field analyzer comprises:

a source application type determiner operative to determine a source application type of said packets.

23. The system according to claim 20, wherein said determining means comprises at least one of:

means for storing and retrieving a source application for a source address from a source application table;

means for determining a source application from a type of service (TOS) packet field; and

means for determining a source application from a differentiated services (DiffServ) header field.

24. The system according to claim 17, wherein said identifier device comprises:

means for storing and retrieving an existing IP flow to and from an IP flow identification data table.

25. The system according to claim 16, wherein said characterizer comprises:

older determining means for determining whether an age of a packet is older than a threshold age;

means for anticipating client application IP flow discards based on said age of said packet;

QoS determining means for determining a QoS requirement for said IP flow; and

means for determining a subscriber identification for one of said one or more subscriber CPE stations associated with said IP flow.

26. The system according to claim 25, wherein said older determining means comprises:

means for analyzing a time to live (TTL) packet-field for determining said age of said packet.

27. The system according to claim 25, wherein said QoS determining means determines said QoS requirement based on at least one of:

a source address;

a destination address; and

a UDP port number,

wherein said QoS determining means comprises:

means for storing and retrieving a QoS requirement for an IP flow from an IP flow QoS requirement table.

28. The system according to claim 1, wherein said classifier comprises:

classifying means for classifying a packet of a new IP flow into a QoS class grouping of a previously classified IP flow.

29. The system according to claim 28, wherein said classifying means comprises:

means for determining and taking into account QoS class groupings of said previously classified IP flow.

30. The system according to claim 29, wherein said classifying means comprises:

means for taking into account any optional differentiated services (Diff Serv) field priority marking for said previously classified IP flow.

31. The system according to claim 29, wherein said classifying means comprises:

means for taking into account any optional type of service (TOS) field priority marking for said previously classified IP flow.

32. The system according to claim 16, wherein said prioritizer device comprises:

means for taking into account hierarchical class based priorities (HCBPs) for said IP flow.

33. The system according to claim 16, wherein said prioritizer device comprises:

means for taking into account virtual private network (VPN) priorities for said IP flow.

34. The system according to claim 16, wherein said prioritizer device comprises:

means for taking into account service level agreement (SLA) based priorities for said IP flow.

35. The system according to claim 16, wherein said prioritizer device comprises:

means for taking into account any type of service (TOS) priorities for said IP flow.

36. The system according to claim 16, wherein said prioritizer device comprises:

means for taking into account any differentiated services (DiffServ) priorities for said IP flow.

37. The system according to claim 16, wherein said identifier comprises:

packet analyzing means for analyzing one or more header and payload packet fields in said IP flow; and

distinguishing means for distinguishing between a new and an existing IP flow.

38. The system according to claim 37, wherein said packet analyzing means is located at each of said one or more subscriber CPE stations for an uplink wireless communication from said each of said one or more subscriber CPE stations to said wireless base station.

39. The system according to claim 37, wherein said distinguishing means is located at each of said one or more subscriber CPE stations for an uplink wireless communication from said each of said one or more subscriber CPE stations to said wireless base station.

40. The system according to claim 37, wherein said packet analyzing means is located at said wireless base station for a downlink wireless communication from said wireless base station to each of said one or more subscriber CPE stations.

41. The system according to claim 37, wherein said distinguishing means is located at said wireless base station for a downlink wireless communication from said wireless base station to each of said one or more subscriber CPE stations.

42. The system according to claim 37, wherein said packet analyzing means comprises:

means for buffering packets of a plurality of IP flows;

extracting means for extracting data from said packet fields of each of said packets; and

second analyzing means for analyzing said packet fields.

43. The system according to claim 42, wherein said extracting means comprises:

means for determining whether said packets are a packet version LPv.4 or IPv.6; and

means for parsing said packet fields of said plurality of IP flows.

44. The system according to claim 42, wherein said second analyzing means comprises:

determining means for determining a source application type.

45. The system according to claim 44, wherein said determining means comprises:

means for storing and retrieving a source application type to and from a source application table.

46. The system according to claim 44, wherein said determining means comprises:

means for determining a source application from a type of service (TOS) packet field.

47. The system according to claim 44, wherein said determining means comprises:

means for determining a source application from a differentiated services (DiffServ) packet field.

48. The system according to claim 44, wherein said determining means comprises:

means for determining a source application from information provided by a direct application conduit.

49. The system according to claim 37, wherein said distinguishing means comprises:

means for storing and retrieving identification information for an existing IP flow to and from an IP flow identification data table.

50. The system according to claim 16, wherein said identifier comprises:

determining means for determining whether said IP flow is known to the system based on a packet received over said shared wireless bandwidth; and

source identifying means for identifying a source application having transmitted said received packet.

51. The system according to claim 50, wherein said determining means is located at said wireless base station for a downlink wireless communication from said wireless base station to said one or more subscriber CPE stations.

52. The system according to claim 50, wherein said determining means is located at each of said one or more subscriber CPE stations for an uplink wireless communication from said each of said one or more subscriber CPE stations to said wireless base station.

53. The system according to claim 50, wherein said identifying means is located at said wireless base station for a downlink wireless communication from said wireless base station to said one or more subscriber CPE stations.

54. The system according to claim 50, wherein said identifying means is located at each of said one or more subscriber CPE stations for an uplink wireless communication from said each of said one or more subscriber CPE stations to said wireless base station.

55. The system according to claim 50, wherein said determining means comprises:

means for buffering said packet;

means for extracting identification information from one or more header and payload packet fields of said packet;

means for performing a lookup of an existing IP flow identifier using said identification information in an existing IP flow data table to determine whether the IP flow is known to the system.

56. The system according to claim 50, wherein said source identifying means comprises:

means for buffering said packet;

means for extracting information from one or more header and payload packet fields of said packet;

means for performing a lookup of a source application type using said information in a source application data table to identify said source application.

57. The system according to claim 16, wherein said characterizer comprises:

age determining means for determining whether an age of a packet is older than a threshold age.

58. The system according to claim 57, wherein said age determining means comprises:

means for analyzing a time to live (TTL) packet field for determining said age of said packet.

59. The system according to claim 57, wherein said age determining means comprises:

means for anticipating application IP flow discards based on said age of said packet.

60. The system according to claim 16, wherein said characterizer comprises:

QoS determining means for determining a QoS requirement for said IP flow if said IP flow is a new IP flow.

61. The system according to claim 16, wherein said characterizer comprises:

means for determining a subscriber CPE identification for said one or more subscriber CPE stations associated with said IP flow if said IP flow is a new IP flow.

62. The system according to claim 60, wherein said QoS determining means comprises:

means for determining QoS requirements based on at least one of:

a source address,

a destination address, and

a UDP port number.

63. The system according to claim 60, wherein said QoS determining means comprises:

means for storing and retrieving a QoS requirement for an IP flow from an IP flow QoS requirement table.

64. The system according to claim 16, wherein said classifier comprises:

means for associating a packet of an existing IP flow with said IP flow.

65. The system according to claim 16, wherein said classifier comprises:

a QoS grouping device operative to group a packet of a new IP flow into a QoS class grouping.

66. The system according to claim 3, wherein said QoS grouping device comprises:

a determining device operative to determine and take into account QoS class groupings for said IP flow.

67. The system according to claim 66, wherein said QoS grouping device comprises:

an optional differentiated services (Diff Serv) device operative to take into account an optional Diff Servs field priority marking for said IP flow.

68. The system according to claim 66, wherein said QoS grouping device comprises:

an optional type of service (TOS) device operative to take into account any optional type of service (TOS) field priority marking for said IP flow.

69. The system according to claim 16, wherein said prioritizer comprises:

a hierarchical class based priority (HCBP) prioritizer operative to prioritize said IP flow based on a HCBP priority of said IP flow.

70. The system according to claim 69, wherein said HCBP prioritizer comprises:

a class based priority limits operative to establish limits for each of said HCBP priorities.

71. The system according to claim 16, wherein said prioritizer device comprises:

a virtual private network (VPN) prioritizer operative to prioritize a plurality of IP flows based on their source being a VPN.

72. The system according to claim 71, wherein said virtual private network (VPN) prioritizer grants preferential priority to said plurality of IP flows associated with said VPN.

73. The system according to claim 71, wherein said virtual private network (VPN) prioritizer grants preferential priority to at least one of:

said VPN IP flows of a particular IP flow type, and

said VPN IP flows from a type of VPN.

74. The system according to claim 73, wherein said type of VPN comprises:

a directory enabled networking (DEN) table management scheme type.

75. The system according to claim 16, wherein said prioritizer device comprises:

a service level agreement (SLA) based prioritizer operative to prioritize said IP flow based on an SLA level of a subscriber source of said IP flow.

76. The system according to claim 75, wherein said SLA level comprises at least one of a premium level, a standard level and a value level.

77. The system according to claim 16, wherein said prioritizer device comprises:

a type of service (TOS) prioritizer that prioritizes said IP flow based on a TOS marking of a packet of said IP flow.

78. The system according to claim 16, wherein said prioritizer device comprises:

a differentiated services (DiffServ) prioritizer that prioritizes said IP flow based on a DiffServ marking of a packet of said IP flow.

79. The system according to claim 16, wherein said prioritizer device comprises:

a weighted fair priority (WFP) prioritizer that ensures fair distribution of said shared bandwidth, that sets reservation policy limits based on IP flow priorities.

80. The system according to claim 75, wherein said SLA based prioritizer comprises:

means for analyzing said SLA level for said IP flow.

81. The system according to claim 80, comprising:

means for prioritizing said IP flow based on one or more subscriber-defined parameters.

82. The system according to claim 75, wherein said SLA level comprises at least one of:

a premium service level;

a normal service level; and

a value service level.

83. The system according to claim 75, wherein said SLA level is used to provide at least one of:

differing traffic rates between SLA subscribers;

network availability for said SLA subscribers;

increased bandwidth for said SLA subscribers;

decreased error rates for said SLA subscribers;

latency guarantees for said SLA subscribers; and

jitter guarantees for said SLA subscribers.

84. The system according to claim 1, wherein said resource allocation means comprises:

assigning means for assigning future slots of a transmission frame to a data packet in the transmission frame for transmission over said wireless medium.

85. The system according to claim 84, wherein said assigning means comprises:

means for applying an advanced reservation algorithm;

first reserving means for reserving a first slot for a first data packet of said IP flow in a future transmission frame based on said advanced reservation algorithm; and

second reserving means for reserving a second slot for a second data packet of said IP flow in a transmission frame subsequent in time to said future transmission frame based on said advanced reservation algorithm,

wherein said second data packet is placed in said second slot in an isochronous manner to the placement of said first data packet in said first slot.

86. The system according to claim **85**, wherein there is a periodic variation between the placement of said first data packet in said first slot and the placement of said second data packet in said second slot.

87. The system according to claim **85**, wherein there is an aperiodic variation between the placement of said first data packet in said first slot and the placement of said second data packet in said second slot.

88. The system according to claim **85**, wherein said advanced reservation algorithm determines whether said IP flow is jitter-sensitive.

89. The system according to claim **1**, wherein said resource allocation means comprises:

means for accounting for hierarchical class based priorities (HCBPs) for said IP flow.

90. The system according to claim **1**, wherein said resource allocation means comprises:

means for accounting for virtual private network (VPN) priorities for said IP flow.

91. The system according to claim **1**, wherein said resource allocation means comprises:

means for accounting for service level agreement (SLA) based priorities for said IP flow.

92. The system according to claim **1**, wherein said resource allocation means comprises:

means for accounting for any type of service (TOS) priorities for said IP flow.

93. The system according to claim **1**, wherein said resource allocation means comprises:

means for accounting for any differentiated services (DiffServ) priorities for said IP flow.

94. The system according to claim **85**, further comprising:

means for providing a periodic variation between the placement of said first data packet in said first slot and the placement of second data packet in said second slot.

95. The system according to claim **85**, further comprising:

means for providing an aperiodic variation between the placement of said first data packet in said first slot and the placement of second data packet in said second slot.

96. The system according to claim **85**, wherein said advanced reservation algorithm comprises:

means for determining whether said IP flow is jitter-sensitive.

97. The system according to claim **85**, comprising: means for providing no periodic variation between successive reservations of succeeding slots.

98. The system according to claim **85**, comprising:

means for providing a periodic variation between successive reservations of succeeding slots.

99. The system according to claim **85**, wherein said advanced reservation algorithm comprises:

means for determining whether said IP flow is jitter-sensitive.

100. The system according to claim **16**, wherein said analyzing and scheduling means comprises an analyzer and a scheduler,

wherein said analyzer is operative to identify IP-priority packet IP flow identification information and to classify said IP flow, and

said scheduler is operative to prioritize said IP flow and operative to take into account said IP priority header identification information.

101. The system according to claim **100**, wherein said IP-priority packet IP flow identification information comprises a determiner operative to determine and to take into account QoS class groupings for said IP flow.

102. The system according to claim **100**, wherein said IP-priority packet IP flow identification information comprises a TOS prioritizer operative to account for any optional type of service (TOS) field priority marking.

103. The system according to claim **102**, wherein said type of service (TOS) field priority marking is compatible with Internet Engineering Task Force (IETF) RFC 1992b.

104. The system according to claim **103**, wherein said type of service (TOS) field priority marking is compatible with IETF RFC 1349.

105. The system according to claim **104**, wherein said marking comprises:

a minimize delay marking;

a maximize throughput marking;

a maximize reliability marking;

a minimize monetary cost marking; and

a normal service marking.

106. The system according to claim **100**, wherein said IP-priority packet header IP flow identification information comprises a DiffServ prioritizer operative to account for any optional differential service (Diff Serv) field priority marking.

107. The system according to claim **106**, wherein said Diff Serv field priority marking is compatible with Internet Engineering Task Force (IETF) RFC 2474.

108. The system according to claim **106**, wherein said Diff Serv field priority marking is compatible with IETF RFC 2475.

109. The system according to claim **100**, wherein said IP-priority packet header IP flow identification information comprises means for taking into account any resource reservation protocol (RSVP) messages and objects.

110. The system according to claim **109**, wherein said RSVP protocol messages include any of the following:

path messages;

reservation (Resv);

path teardown messages;

resv teardown messages;

path error messages; and

confirmation messages.

111. The system according to claim **109**, wherein said RSVP protocol objects include any of the following:

null;

session;

RSVP_hop;

time_values;

style;

flowspec;

sender_template;

sender_Tspec;

Adspec;

Error_Spec;

Policy_data;

Integrity;

Scope; and

Resv_Confirm.

112. The system according to claim 106, wherein said RSVP marking is compatible with Internet Engineering Task Force (IETF) RFC 2205.

113. The system according to claim 33, comprising:

means for analyzing said virtual private network (VPN) priorities for said IP flow.

114. The system according to claim 113, comprising:

means for prioritizing all VPN IP flows.

115. The system according to claim 113, comprising:

means for prioritizing said IP flow based on one or more subscriber-defined parameters.

116. The system according to claim 33, wherein said VPN comprises a directory enabled networking (DEN) table management scheme.

117. The system according to claim 33, wherein said VPN is implemented using a point-to-point tunneling protocol (PPTP).

118. The system according to claim 1, wherein said system is used in a point to point (PtP) telecommunications system.

119. The system according to claim 118, wherein said shared wireless bandwidth comprises a wireless communication medium comprising at least one of:

a radio frequency (RF) communications medium;

a cable communications medium; and

a satellite communications medium.

120. The system according to claim 119, wherein said wireless communication medium further comprises, a telecommunications access method including at least one of:

a time division multiple access (TDMA) access method;

a time division multiple access/time division duplex (TDMA/TDD) access method;

a code division multiple access (CDMA) access method; and

a frequency division multiple access (FDMA) access method.

121. The system according to claim 118, wherein said first data network comprises at least one of:

a wireline network;

a wireless network;

a local area network (LAN); and

a wide area network (WAN).

122. The system according to claim 118, wherein said second network comprises at least one of:

a wireline network;

a wireless network;

a local area network (LAN); and

a wide area network (WAN).

123. The system according to claim 118, said resource allocation means comprises a resource allocator that allocates shared bandwidth between said wireless base station and one of said subscriber CPE stations.

124. The system according to claim 123, wherein said resource allocator optimizes end-user internet protocol (IP) quality of service (QoS).

125. The system according to claim 123, wherein said resource allocator is application aware.

126. The system according to claim 1, wherein said system is a broadband coaxial cable telecommunications system wherein said wireless medium comprises a coaxial cable communications medium.

127. The system according to claim 1, wherein the system is a wireless local area network (LAN) point to multi-point (PtMP) system.

128. The system according to claim 1, wherein said wireless base station is a wireless access point.

129. The system according to claim 126, wherein said resource allocation means comprises a coaxial cable resource allocator for allocating shared bandwidth between said wireless base station and said subscriber CPE stations.

130. The system according to claim 129, wherein said coaxial cable resource allocator optimizes end-user internet protocol (IP) quality of service (QoS).

131. The system according to claim 126, wherein said coaxial cable communications medium comprises a radio frequency data communication over a coaxial cable, wherein one or more cable modems modulate and demodulate signals transmitted over said coaxial cable communications medium.

132. The system according to claim 131, wherein said cable modem is DOC/SYS compliant.

133. The system according to claim 130, wherein said end-user IP QoS optimized coaxial cable resource allocator system comprises:

an IP flow identifier;

an IP flow characterizer;

an IP flow classifier; and

an IP flow prioritizer.

134. The system according to claim 129, wherein said coaxial cable communications medium comprises, a telecommunications access method including at least one of:

a time division multiple access (TDMA) access method;

a time division multiple access/time division duplex (TDMA/TDD) access method;

a code division multiple access (CDMA) access method; and

frequency division multiple access (FDMA) access method.

135. The system according to claim 126, wherein said first data network comprises at least one of:

a wireline network;

a wireless network;

a local area network (LAN); and

a wide area network (WAN).

136. The system according to claim 126, wherein said second network comprises at least one of:

a wireline network;

a wireless network;

a local area network (LAN); and

a wide area network (WAN).

137. The system according to claim 129, wherein said coaxial cable resource allocator is application aware.

138. The system according to claim 129, wherein the system is used in a point to point (PtP) network.

139. The system according to claim 1, wherein said resource allocation means is a part of a media access control (MAC) layer.

140. The system according to claim 9, wherein said wireless communication medium further comprises a telecommunications access method comprising a time division multiple access/time division duplex (TDMA/TDD) access method and wherein the system further comprises a TDMA/TDD media access control (MAC) transmission frame, comprising:

one or more dynamically allocatable IP flow control slots for providing IP flow control information over a wireless medium between said wireless base station and said one or more subscriber customer premises equipment (CPE) stations; and

one or more dynamically allocatable IP flow data slots for providing IP flow data information over said wireless communication medium between said wireless base station and said one or more subscriber customer premises equipment (CPE) stations.

141. The system according to claim **140**, wherein said control slots comprise at least one of:

a downstream acknowledgment slot;

a reservation request slot;

an operations data slot;

an upstream acknowledgment slot;

an acknowledgment request slot;

a frame descriptor slot; and

a command and control slot.

142. The system according to claim **140**, wherein said data slots comprise at least one of:

uplink data slots for transmission in an uplink direction from each of said one or more subscriber CPE stations to said wireless base station; and

downlink data slots for transmission in a downlink direction from said wireless base station to each of said one or more subscriber CPE stations.

143. The system according to claim **140**, wherein said time division multiple access/time division duplex (TDMA/TDD) transmission media access method involves:

a downlink subframe for use over said wireless medium from said wireless base station and said one or more subscriber customer premises equipment (CPE) stations; and

an uplink subframe for use over said wireless medium from said subscriber CPE stations to said wireless base station,

wherein a bandwidth is dynamically allocated between said downlink subframe and said uplink subframe for transmission of Internet protocol (IP) flow information so as to optimize end-user IP quality of service (QOS).

144. The system according to claim **143**, wherein multiple slots in said downlink subframe are scheduled for one of said one or more subscriber CPE stations for a single internet protocol (IP) flow.

145. The system according to claim **143**, wherein multiple slots in said downlink subframe are scheduled for one of said one or more subscriber CPE stations for a plurality of Internet protocol (IP) flows.

146. The system according to claim **143**, wherein multiple slots in said uplink subframe are scheduled for one of said one or more subscriber CPE stations for a single internet protocol (IP) flow.

147. The system according to claim **143**, wherein multiple slots in said uplink subframe are scheduled for one of said one or more subscriber CPE stations for a plurality of internet protocol (IP) flows.

148. The system according to claim **143**, further comprising:

one or more dynamically allocatable reservation request contention slots for addressing contentions between reservation requests for available slots in said uplink subframe between said wireless base station and each of said one or more subscriber CPE stations for transmission of IP flows.

149. The system according to claim **143**, wherein said contention slots are dynamically allocated according to the frequency of detected collisions between said reservation requests.

150. The system according to claim **143**, further comprising:

a frame descriptor block for transmitting one or more reservation slots in said downlink subframe defining where each of said one or more subscriber CPE stations requesting a reservation will place uplink data thereof.

151. The system according to claim **140**, wherein said IP flow control slots comprise at least one of:

a downstream acknowledgment slot;

an operations data slot;

an upstream acknowledgment slot;

an acknowledgment request slot; and

a frame descriptor slot.

152. The system of claim **1**, further comprising a TCP adjunct system that prevents operation of a transmission control program (TCP) sliding window algorithm that controls a TCP transmission rate in said packet-centric wireless point to multi-point telecommunications system, said TCP adjunct system comprising:

a TCP adjunct agent that takes into account application awareness, guarantees enduser quality of service (QoS), and prevents operation of a TCP sliding window algorithm that controls a TCP transmission rate in a manner that optimizes for a wireless communication medium.

153. The system of claim **152**, wherein said TCP adjunct agent obviates modification of a source TCP layer at a first of said one or more host workstations and a destination TCP layer at one of said one or more subscriber workstations.

154. The system of claim **153**, wherein said source and destination TCP layers are unaware of operation modification by said TCP adjunct agent.

155. The system of claim **152**, wherein said TCP adjunct agent is configured to intercept retransmission requests between a TCP layer of one of said subscriber workstations coupled to a first subscriber CPE station and a TCP layer of at least one of a host workstation and said wireless base station.

156. An IP flow classification system that groups IP flows in a packet-centric wireless point to multi-point telecommunications system, said classification system comprising:

a wireless base station coupled to a first data network;

one or more host workstations coupled to said first data network;

one or more subscriber customer premise equipment (CPE) stations in wireless communication with said wireless base station over a shared wireless bandwidth using a packet-centric protocol over a wireless communication medium;

one or more subscriber workstations coupled to each of said subscriber CPE stations over a second network;

a resource allocator operative to optimize end-user quality of service (QoS) and allocating shared bandwidth among said subscriber CPE stations; and

an analyzer and scheduler operative to analyze and schedule an internet protocol (IP) flow over said shared wireless bandwidth, wherein said analyzer and scheduler comprises:

a classifier that classifies said IP flow.

157. The system of claim **156**, wherein said classifier comprises:

an association device that associates a packet of an existing IP flow with said IP flow.

158. The system of claim **156**, wherein said classifier comprises:

QoS grouping device that groups a packet of a new IP flow into a QoS class grouping.

159. The system of claim 158, wherein said QoS grouping device comprises:

determining device that determines and takes into account QoS class groupings for said IP flow.

160. The system of claim 159, wherein said QoS grouping device comprises:

optional differentiated services (Diff Serv) device that takes into account an optional Diff Servs field priority marking for said IP flow.

161. The system of claim 159, wherein said QoS grouping device comprises:

optional type of service (TOS) device that takes into account any optional type of service (TOS) field priority marking for said IP flow.

162. The system according to claim 156, wherein the wireless point to multi-point telecommunications system is a wireless local area network (LAN) system.

163. The system according to claim 156, wherein the wireless point to multi-point telecommunications system is a wireless wide area network (WAN) system.

* * * * *